ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 336/346

ОЦЕНКА УГРОЗ БЕЗОПАСНОСТИ СЕТЕЙ ПОКОЛЕНИЯ 5G В РЕАЛЬНЫХ СЕТЯХ

Ахунжанов Ислам Бахадырович,
аспирант, islam.ahunjanov@gmail.com

Акбарова Адиля Нурлановна,
аспирант,akbarovaa94@gmail.com,

Кыргызский государственный технический университет имени Исхак Раззакова

Аннотация

Достижения в сетях мобильной связи от 2G до 5G привели к беспрецедентному росту трафика, и ожидается, что сети мобильной связи 5G будут использоваться в различных отраслях промышленности на основе инновационных технологий, быстрых не только с точки зрения чрезвычайно низкой задержки, но и устройств массового доступа. Различные типы услуг, такие как расширенная мобильная широкополосная связь (eMBB), массовая связь машинного типа (mMTC) и сверхнадежная связь с малой задержкой (uRLLC), представляют собой увеличение числа атак на личную информацию пользователей, конфиденциальную информацию. и информация о конфиденциальности. Поэтому оценка безопасности необходима для проверки и противодействия этим различным атакам. В этом исследовании мы изучили предысторию и проблемы сетей мобильной связи 5G для изучения существующих уязвимостей и оценили текущую ситуацию путем оценки угроз безопасности 5G в реальных мобильных сетях, находящихся в эксплуатации.

Ключевые слова: Мобильная связь 5G; Мобильная сеть; NAS; SIP; Тестирование безопасности 5G.

ASSESSMENT OF THE SECURITY THREATS OF THE 5G GENERATION NETWORKS IN REAL NETWORKS

Islam B. Ahunjanov,
graduate student, islam.ahunjanov@gmail.com,

Adilya N. Akbarova,
graduate student, akbarovaa94@gmail.com,

Kyrgyz State Technical University named after Iskhak Razzakov

ABSTRACT

Advances in mobile communication networks from 2G to 5G have brought unprecedented traffic growth, and 5G mobile communication networks are expected to be used in a variety of industries based on innovative technologies, fast not only in terms of extremely low latency but massive access devices. Various types of services, such as enhanced mobile broadband (eMBB), massive machine type communication (mMTC), and ultra-reliable and low latency communication (uRLLC), represent an increase in the number of attacks on users' personal information, confidential information, and privacy information. Therefore, security assessments are essential to verify and cope with these various attacks. In this research, we looked at 5G mobile communication network backgrounds and problems to investigate existing vulnerabilities and assessed the current situation through evaluation of 5G security threats in real-world mobile networks in service.

Keywords: Mobile communication 5G; Mobile network; NAS; SIP; 5G security testing.

В феврале 2017 года Международный союз электросвязи (МСЭ) выпустил отчет, в котором установлены ключевые требования, которые представляют собой минимальные требования, связанные с техническими характеристиками для IMT-2020 для технологии мобильной связи 5G. В этом отчете запрашивается минимальная пропускная способность 1 ГГц, максимальная скорость передачи данных 20 Гбит/с и минимальное время задержки 1 мс для услуг следующего поколения. Это технические требования для реализации ключевых целей 5G: суперсвязь, сверхбыстрая и сверхмалая задержка, а также минимальные требования для реализации различных услуг 5G.

Мобильная связь 5G является более инновационной по сравнению с мобильной связью 4G в целом, включая скорость, использование протокола и конфигурации сети. Беспроводная сеть 5G настроена на программно определяемую сеть (SDN) со скоростью 20 Гбит/с, что в 20 раз быстрее, чем существующая долгосрочная эволюция (LTE), в то время как базовая сеть 5G была изменена с централизованного типа на децентрализованный тип, чтобы минимизировать задержку передачи трафика [2].

В связи с такими техническими изменениями МСЭ-R определил услуги 5G. Он классифицировал услуги 5G на расширенную мобильную широкополосную связь (eMBB), где скорость является ключевым элементом, массовую связь машинного типа (mMTC), где ключевым элементом является пропускная способность, и сверхнадежную связь с малой задержкой (uRLLC), где требуется минимизация времени задержки. и настроил услуги для использования инфраструктуры 5G в промышленной среде во всем обществе.

Технические стандарты 5G определяются проектом партнерства 3-го поколения (3GPP), а выпуск 15, замороженный в марте 2019 года, определяет архитектуры неавтономных (NSA) и автономных (SA) и охватывает миграцию системы LTE. Кроме того, выпуск 16, замороженный в июле 2020 года, охватывает отраслевую поддержку конвергенции на основе 5G, включая связь 5G-транспортное средство со всем (V2X) и Интернет вещей 5G (IoT), а также улучшения производительности в системе 5G. В выпуске 17, который будет заморожен в марте 2022 года, идет стандартизация с целью расширения покрытия 5G, передачи небольших данных и использования нелицензируемых диапазонов. Кроме того, поскольку продажи отраслей, связанных с 5G, растут, ожидается, что продажи инфраструктуры беспроводных сетей 5G достигнут 6,8 млрд долларов США в 2021 году, согласно отчетам, опубликованным Gartner, как показано в таблице 1.

Segment	2020 Revenue	2021 Revenue	2022 Revenue
5G	13,768.0	19,128.9	23,254.6
LTE and 4G	17,127.8	14,569.1	12,114.0
3G and 2G	3,159.6	1,948.2	1,095.2
Small Cells Non-5G	6,588.5	7,117.9	7,113.9
Mobile Core	5,714.6	6,056.2	6,273.3
Total	**46,358.5**	**48,820.2**	**49,851.0**

Source: Gartner (August 2021)

В этом контексте растет количество голосов пользователей, призывающих к безопасной среде обслуживания 5G, и перед запуском услуг требуется множество проверок из-за возможности внутренних угроз безопасности в существующей сети связи LTE. Кроме того, необходимо заблаговременно выявлять новые угрозы безопасности 5G из-за технических изменений, отличающихся от 4G, и при необходимости необходимо повышать безопасность услуг путем разработки технологии безопасности, предназначенной для 5G [6].

Кроме того, ожидается, что масштабы мирового рынка безопасности 5G вырастут на 50 % совокупного годового темпа роста (CAGR) примерно до 4 млрд долларов США в 2023 году и около 7 млрд долларов США в 2025 году. В частности, более 95% рынок безопасности 5G занимает область защитных решений. В последнее время о серьезных угрозах безопасности сообщают такие статьи, как Hongil Kim et al. и Мерлин Хлоста и др. Однако большинство операторов мобильной связи (операторы услуг 5G) предоставляют услуги 5G без применения методов реагирования, связанных с угрозами безопасности.

Вклад этого документа заключается в следующем, и основной вклад заключается в том, что мы даем представление о том, какие проблемы безопасности действительны в реальной сети 5G NSA и как их можно смягчить.

Мы разделили угрозы безопасности 5G NSA на сеть радиодоступа (RAN) и базовую сеть (CN), чтобы создать дерево атак и разработать 15 тестовых сценариев, которые можно применить к реальным сетям.

Мы проверили разработанные 15 тестовых случаев в реальных сетях трех операторов мобильной связи и выявили восемь действительных уязвимостей.

Из этих восьми действительных уязвимостей мы предложили исправления программного обеспечения PKG для оборудования или изменения конфигурации для пяти и соответствующие контрмеры для оставшихся трех.

С точки зрения традиционной сетевой безопасности сеть мобильной связи представляет собой очень труднодоступную инфраструктуру. О такой недоступности можно говорить в трех аспектах, и первый из них — сложная конфигурация сети. Сети мобильной связи можно условно разделить на секции беспроводной сети, базовой сети и сети взаимосвязи, а протоколы и интерфейсы, используемые в каждой секции, различаются [1]. Это означает, что для каждого раздела необходимо применять и управлять различными технологиями безопасности. Кроме того, существует так много разделов, что точки мониторинга безопасности усложняются, а анализ трафика для поиска угроз безопасности неизбежно затруднен.

Во-вторых, терминалы используют частный адрес интернет-протокола (IP), в отличие от обычных сетей. Поскольку IP-адрес терминала меняется всякий раз, когда терминал получает доступ к сети мобильной связи, даже если обнаружена угроза безопасности, очень сложно идентифицировать злоумышленника, вызвавшего эту угрозу [1].

Последним является использование выделенных протоколов. Существует ограничение на повышение стабильности за счет использования существующего оборудования безопасности, которое не может интерпретировать выделенные протоколы, поскольку оно использует протоколы, используемые только в сетях мобильной связи, такие как прикладной протокол NG (NGAP), уровень отсутствия доступа (NAS), протокол туннелирования GPRS (GTP), диаметр и протокол управления пересылкой пакетов (PFCP), а не общий протокол управления передачей (TCP)/IP. В частности, поскольку сеть мобильной связи 5G использует разные выделенные протоколы базовой сети как в конфигурациях NSA, так и в SA, требования безопасности неизбежно различаются в зависимости от конфигурации сети.

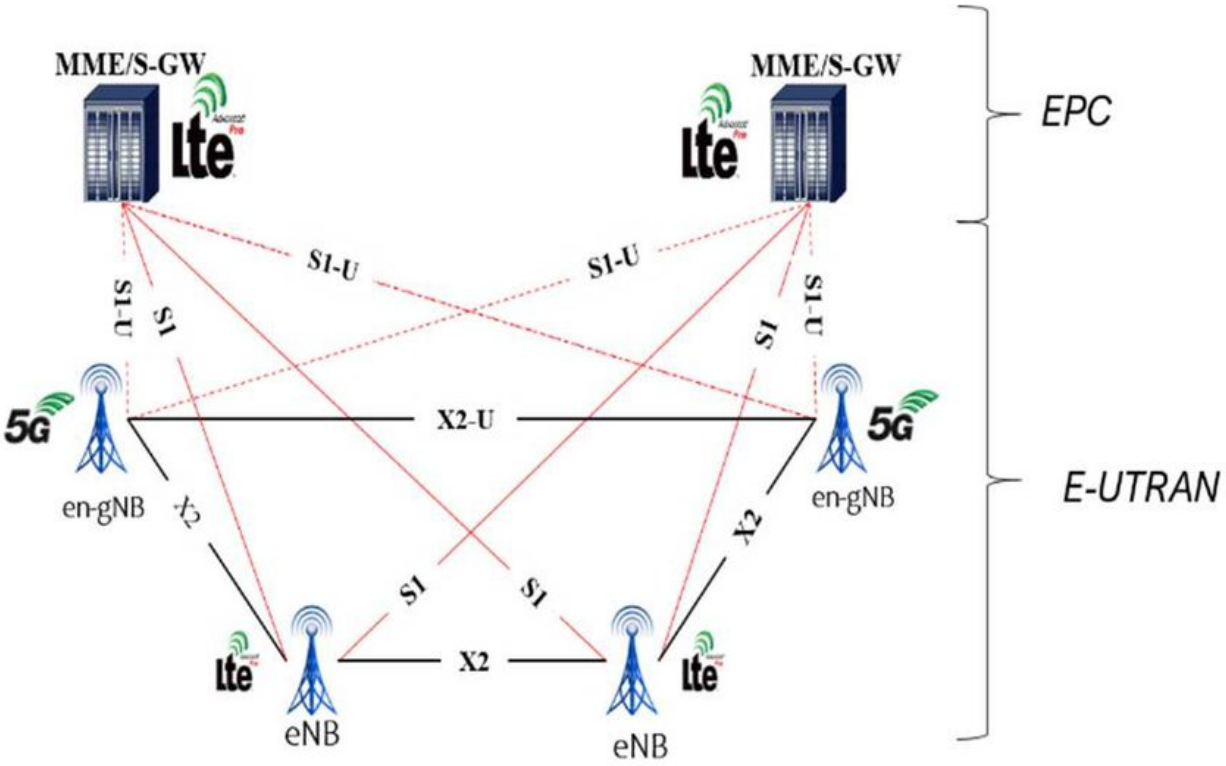

Рис.1. Архитектура сети 5G NSA

5G NSA — это метод, при котором базовая сеть настраивается как усовершенствованное пакетное ядро (EPC) на основе LTE, а усовершенствованный узел B (eNB) и узел B следующего поколения (gNB) используются вместе для беспроводных сетей. Учитывая, что с точки зрения операторов мобильной связи, предоставляющих существующие услуги LTE, сложно быстро внедрить метод SA 5G, для услуг 5G в этой архитектуре несложно выполнить «мягкую посадку».

Секция связи 5G NSA разделена на беспроводную секцию и проводную секцию, как показано на рисунке 1. Беспроводная секция представляет собой RAN между пользовательским оборудованием (UE) и базовой станцией, а проводная секция представляет собой CN между базовой станцией и сервисной сетью. Здесь существует плоскость управления (CP) между терминалом и RAN или CN, в то время как существует плоскость пользователя (UP) между терминалом и сетью IP-мультимедийной подсистемы

(IMS) для Интернета или голосовых услуг. В CP передается трафик с использованием таких протоколов, как управление радиоресурсами (RRC), NAS и GTP-C, в то время как туннелируемый трафик с использованием протокола GTP-RRC в пользовательских данных, таких как голос, передается в UP. На рис. 1 показана архитектура 5G NSA с упрощенной конфигурацией, основанной на компонентах, требуемых в этом документе. Описания каждого компонента в 5G NSA приведены ниже [3].

- организацию интерфейсов плоскости управления N1, N2;
- организацию обменом сигнализации NAS через интерфейс N1, шифрование и защита целостности сигнализации NAS;
- управление регистрацией пользовательского терминала (UE) в сети и контроль возможных состояний регистрации (RM-DEREGISTERED, RM-REGISTERED);
- управление соединением пользовательского терминала (UE) с сетью и контроль возможных состояний соединения (CM-IDLE, CM-CONNECTED);
- управление доступностью пользовательского терминала (UE) в сети в состоянии CM-IDLE;
- управление мобильностью пользовательского терминала (UE) в сети в состоянии CM-CONNECTED;
- передачу коротких сообщений между оборудованием пользователя (UE) и SMF;
- управление службами определения местоположения;
- передачу сообщений между UE и функцией управления местоположением LMF (Location Management Function), а также между RAN и LMF;
- выделение идентификатора потока данных EPS (Evolved Packet System) для взаимодействия с EPS;
- взаимодействие с неопределенными стандартами 3GPP сетями доступа посредством модуля взаимодействия N3IWF (Non-3GPP InterWorking Function).

Как и в случае с NSA, при доступе к сетевой безопасности 5G SA следует учитывать новые технические элементы. Беспроводные сети, называемые 5G NR, изменили форму конфигурации с существующей конфигурации радиоблока (RU) и цифрового блока (DU) на конфигурацию блока доступа (AU), DU и центрального блока (CU). В AU к существующему RU добавляется физический уровень и применяется метод связи с дуплексной связью с временным разделением (TDD). Кроме того, из-за облачности DU, CU недавно введен и берет на себя роль оркестровки. Наряду с изменениями в беспроводных сетях базовые сети перешли на децентрализованную конфигурацию, чтобы разделить CP и UP и минимизировать задержку передачи трафика. Таким образом, для обеспечения безопасности основной сети следует рассматривать децентрализованную конфигурацию безопасности, а не существующую централизованную конфигурацию. Требования безопасности для сетей мобильной связи 5G, требующих суперподключения, сверхбыстрой и сверхнизкой задержки, значительно расширяются [3].

Типы угроз безопасности базовой сети

Тип.1. Утечка информации: информацию о базовых сетях 5G NSA можно в значительной степени разделить на информацию об оборудовании EPC для обработки данных и информацию об оборудовании IMS для предоставления различных услуг.

Поскольку оборудование EPC взаимодействует с использованием протокола GTP, а оборудование IMS взаимодействует с использованием протокола SIP, злоумышленник может выбрать протокол, подходящий для получения необходимой информации. Протокол GTP делится на GTP-C, используемый между оборудованием базовой сети, и GTP-U, который доставляет трафик данных в пользовательский терминал через туннель между базовой станцией и PGW. Чтобы узнать информацию об IP-адресе оборудования EPC, злоумышленник может использовать метод внедрения пакетов, который загружает эхо-запрос, сообщение GTP-C для проверки работоспособности между оборудованием базовой сети, в полезных данных для отправки. При запуске команды отладочного моста Android (ADB) в терминале Android с помощью программы Packit создается пакет, и при отправке пакета в IP-диапазон, идентифицированный с помощью Tracert в состоянии привязки, пакет GTP-C вводится и передается на сеть мобильной связи. PGW проверяет это и отправляет эхо-ответ, где злоумышленник может определить, что IP-адрес источника этого сообщения является IP-адресом PGW [5].

Тип.2. Истощение IP-адресов: метод внедрения пакетов, описанный ранее для провоцирования угрозы утечки информации, называется GTP-in-GTP, и злоумышленник может истощить пулы IP-адресов, выделенные для терминалов в базовой сети, с помощью того же метода. В то время как эхо-запрос GTP-C, который играет роль эхо-запроса, используется для получения IP-адреса для оборудования базовой сети, запрос создания сеанса GTP-C вводится и отправляется в базовую сеть для выделения IP-адреса терминалу. Злоумышленник может последовательно увеличивать номер терминала в запросе на создание сеанса, чтобы PGW выделил несколько IP-адресов. Если PGW выделяет все доступные IP-адреса, запросы на создание сеанса от обычных терминалов будут отклонены, и все терминалы, имеющие доступ к этой базовой сети, не смогут обмениваться данными.

Тип.3. DoS: Злоумышленник может непрерывно отправлять сообщение с запросом на подключение для доступа к сети 5G NSA, настроив несколько терминалов в качестве бот-сетей и повторяя включение и выключение режима полета. Это может вызвать чрезмерную нагрузку трафика на опорную сеть определенного оператора мобильной связи. Один запрос на присоединение может создать максимум восемь сообщений GTP-C, что в 8 раз увеличивает объем трафика для функции CN в базовой сети пропорционально одной злонамеренной манипуляции, совершенной злоумышленником

Тип.4. Манипуляция NAS: из сообщений протокола NAS для передачи сигналов между терминалами и базовой сетью сообщения запроса на присоединение, используемые на начальном этапе присоединения, не имеют гарантированного шифрования или целостности. Поэтому злоумышленник может установить мошенническую базовую станцию рядом с жертвой, чтобы украсть эти сообщения и манипулировать ими. В частности, сообщение-запрос на присоединение имеет поле возможностей сети UE, которое может устанавливать шифрование или целостность для всех данных, полученных или переданных терминалом. Злоумышленник может манипулировать значениями в EEA, которое представляет собой поле для передачи алгоритма шифрования, выбранного терминалом, и EIA, которое представляет собой поле для передачи алгоритма проверки целостности, выбранного терминалом, в поле сетевых возможностей UE. Техническая спецификация 3GPP (TS.) 33.401 определяет основное использование алгоритма проверки целостности в терминалах, но определяет выборочное использование алгоритма шифрования. На самом деле результаты испытаний, проведенных Рурским университетом в Германии в 2019 году на пяти европейских странах и 12 перевозчиках, показали, что четыре из 12 перевозчиков не позволяют использовать даже ту целостность, которую необходимо использовать.

Тип.5. Подслушивание: голосовая связь в сети 5G использует сеть IMS и инициирует сеанс по протоколу SIP в соответствии со стандартом 3GPP. Поэтому безопасность в протоколе SIP очень важна и обеспечивается в основном с помощью ассоциаций безопасности (SA) безопасности интернет-протокола (IPSec). Тем не менее, IPSec SA также выборочно выполняется операторами сетей 5G, и поддержка передачи голоса по LTE (VoLTE) не означает поддержку всего IPSec из-за его значительного влияния на производительность терминала. Модель Samsung Galaxy S10, недавно выпущенный 5G-терминал, также поддерживает IPSec, но есть проблема, при которой рассматриваемую настройку можно отключить через скрытое меню. Если злоумышленник может удаленно получить доступ к скрытому меню жертвы и изменить настройку IPSec, вызов жертвы будет передаваться без шифрования. Если поле EEA изменено с помощью манипуляций с NAS, описанных выше, и алгоритм шифрования NAS не используется, беспроводная связь в разделе AS также не шифруется. В этой ситуации злоумышленник может прослушивать беспроводной трафик в форме «человек посередине» (MitM) и прослушивать незашифрованный голосовой трафик жертвы как есть.

Тип.6. Спуфинг: IP-спуфинг — типичная сетевая атака. Если злоумышленник меняет IP-адрес трафика данных, передаваемого из каждой сети 5G, на IP-адрес жертвы и отправляет трафик данных, все его ответы доставляются жертве, что может привести к недействительной тарификации и даже отказу в обслуживании. Кроме того, спуфинг SIP или MMS может быть использован для голосового фишинга. Когда заголовок «от», который указывает исходящий номер в заголовке пакета SIP, является фальсифицированным, входящий терминал отображает этот фальсифицированный номер [5].

Контрмеры посредством стандартизации

DoS пользователя (DoS соединения RRC). Основная причина угрозы DoS-соединения RRC-соединения заключается в том, что запрос RRC-соединения, сообщение, передаваемое, когда пользовательский терминал получает доступ к сети, передается в виде открытого текста, и сообщение включает TMSI, временную идентификационную информацию пользовательского терминала. Чтобы отреагировать на это, подделка RRC-сообщений должна быть проверена на уровне базовой станции, что нелегко определить в 3GPP. Кроме того, блокирование злоумышленниками возможности узнать временную идентификационную информацию конкретного пользователя может быть способом проверки, что также непросто, поскольку существует слишком много известных методов. Использование временной идентификационной информации в запросе на подключение RRC предназначено для предотвращения вторжения в частную жизнь, вызванного утечкой и злоупотреблением IMSI, который является информацией идентификации абонента в USIM, но злоумышленники могут перехватывать сообщения запроса на подключение RRC, отправленные в виде обычного текста, и легко идентифицировать TMSI, который является временной идентификационной информацией. Благодаря этому злоумышленник может создать и передать модулированное сообщение запроса RRC-соединения, так что базовая станция ошибочно примет это сообщение за сообщение, отправленное UE-жертвой. В базовой сети временная идентификационная информация создается с определенным интервалом времени по определенным правилам на основе IMSI, и даже если TMSI изменен, злоумышленник может идентифицировать измененный TMSI и снова создать сообщение об атаке. При получении модулированного запроса RRC-соединения базовые станции отменяют соединение с существующим терминалом жертвы, не проверяя статус модуляции, и разрешают доступ к терминалу злоумышленника. В такой ситуации, если базовая станция не отключается от выходящего терминала жертвы или сохраняет соединение в течение определенного периода времени, это может уменьшить угрозу DoS

жертвы. Поскольку терминал злоумышленника не проходит аутентификацию после установления соединения RRC, поддержание соединения с существующим терминалом только в течение периода, когда терминал злоумышленника отправляет запрос на соединение RRC, а аутентификация завершается неудачно, может незначительно повлиять на производительность базовой станции [4].

NAS Manipulation (подмена шифрования NAS). Стандарт 3GPP 5G поддерживает как проверку целостности, так и шифрованную связь для усиления безопасности протокола NAS между терминалами и опорными сетями 5G. Однако, поскольку шифрованная связь является не обязательной, а дополнительной функцией среди функций безопасности протокола NAS, в некоторых случаях функции безопасности не используются в соответствии с политикой страны или оператора мобильной связи (3GPP TS. 33.401). В дополнение к экстренным вызовам некоторые страны или операторы могут не использовать возможности шифрования, предоставляемые стандартами 5G, с точки зрения безопасности [5].

Кроме того, стандарт 5G не определяет взаимную аутентификацию между терминалами (UE) и сетями 5G или функцию проверки целостности исходных сообщений, которыми обмениваются перед шифрованием, которая основана на базовом доверии, предполагающем, что исходные сообщения не модулируются. Эта проблема возникает из-за уязвимости, которая не подтверждает подделку первого сообщения запроса доступа (запроса на подключение) к сети 5G, отправленного UE. Злоумышленник проникает между UE жертвы и базовой станцией, манипулирует сообщением с запросом на доступ, включая запрос на шифрование и проверку целостности, обычно отправляемое с терминала, в сообщение с запросом на доступ с отключенным шифрованием и непроверенной целостностью, и отправляет его на обычную базу данных [5].

Подслушивание (SIP-спуфинг). Поскольку прослушивание, вызванное SIP-спуфингом, возможно при снятии IPSec, необходимо направить параметры шифрования голосовой связи между терминалами и сетью 5G, чтобы они управлялись сетью оператора мобильной связи, а не обрабатывались в соответствии с функцией терминала (выборочное приложение требуется в сети для терминалов, не поддерживающих IPSec). Если настройка IPSec голосовой службы 5G определяется функцией терминала, злоумышленники могут предпринять несколько атак, используя настройки своего терминала. Кроме того, нам нужны усилия по повышению осведомленности, чтобы предать гласности риск утечки деталей связи, когда злоумышленники злонамеренно модулируют сообщения и участвуют в обмене данными без шифрования между терминалом и сетью 5G. Применимый раздел для IPSec определяется как локальная политика в 3GPP, но необходим пересмотр, чтобы сделать его обязательным на уровне стандарта 3GPP [5].

Заключение

В ходе этого исследования мы выявили различные угрозы безопасности, которые могут возникнуть в сети 5G NSA, проверили их в реальной сети и предложили способы повышения безопасности. Кроме того, мы выявили постоянные уязвимости в существующей системе мобильной сети посредством изучения недавних исследований 5G и рассмотрели потребность в новых методах безопасности, а не в традиционных методах безопасности и соответствующих исследованиях.

Злоумышленник может отключить настройки шифрования между терминалом жертвы и базовой сетью, используя поддельную базовую станцию, чтобы использовать данные жертвы или перехватить содержимое сообщения. Мы реализовали алгоритм для обнаружения этого и провели тесты производительности обнаружения. Анализируя поля шифрования в сообщениях протокола NAS между терминалами и опорными сетями,

можно установить каналы обхода шифрования или определить, являются ли они нестандартными терминалами. Во-первых, организация канала обхода шифрования для обнаружения случаев, когда EEA в поле возможностей сети UE устанавливается как полный шифр (EEA0), когда терминал получает доступ к сети 5G NSA. Во-вторых, хотя изменение возможностей UE в настройках воспроизводимых сетевых возможностей UE на терминале может быть подтверждено для нестандартных терминалов, может быть обнаружен случай, который завершает этап завершения безопасности NAS без отказа от этапа завершения безопасности NAS. В результате разработан план по стандартизации руководств для системы безопасности по обнаружению этих нешифрующих каналов NAS.

Список литературы:

1. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи: учебник для ВУЗов. - СПб.: БХВ-Петербург, 2014. - 400 с.
2. Данилов В.И. Сети и стандарты мобильной связи: учебное пособие. - СПб.: СПбГУТ, 2015. -100 с.
3. Олейникова А.В., Нуртай М.Д., Шманов Н.М. Перспективы развития связи 5G // Современные материалы, техника и технологии, 2015. № 2 (2). [Электронный ресурс]. URL: https://cyberleninka.ru/artide/n/perspektivy-razvitiya-svyazi5g/ (дата обращения: 04.12.2020).
4. Сети 5G: обеспечение конфиденциальности и безопасности [Электронный ресурс]. URL: https://www.lastmile.su/journal/article/9083
5. 5G и кибербезопасность: все, что нужно знать [Электронный ресурс]. URL: https://www.kaspersky.ru/resource-center/threats/5g-pros-and-cons
6. Безопасность 5G: угрозы из прошлого и надежды на будущее [Электронный ресурс]. URL: https://www.iksmedia.ru/articles/5491547-Bezopasnost-5G-ugrozy-iz-proshlogo.html

References:

1. Goldshtein B.S., Sokolov N.A., Yanovsky G.G. Communication networks: textbook for universities. – St. Petersburg: BHV-Petersburg, 2014. – 400 p.
2. Danilov V.I. Networks and standards of mobile communications: textbook. - St. Petersburg: SPbSUT, 2015. -100 p.
3. Oleynikova A.V., Nurtai M.D., Shmanov N.M. Prospects for the development of 5G communications // Modern materials, equipment and technologies, 2015. No. 2 (2). [Electronic resource]. URL: https://cyberleninka.ru/artide/n/perspektivy-razvitiya-svyazi5g/ (access date: 12/04/2020).
4. 5G networks: ensuring privacy and security [Electronic resource]. URL: https://www.lastmile.su/journal/article/9083
5. 5G and cybersecurity: everything you need to know [Electronic resource]. URL: https://www.kaspersky.ru/resource-center/threats/5g-pros-and-cons
6. 5G security: threats from the past and hopes for the future [Electronic resource]. URL: https://www.iksmedia.ru/articles/5491547-Bezopasnost-5G-ugrozy-iz-proshlogo.html