Материалы XXI Международной научной конференции
«ОБЩЕСТВО: НАУЧНО-ОБРАЗОВАТЕЛЬНЫЙ ПОТЕНЦИАЛ РАЗВИТИЯ (идеи, ресурсы, решения)»
(г. Чебоксары, Россия, 31 октября 2022 г.)

ТЕХНИЧЕСКИЕ НАУКИ

УДК 621.37К

ЭТАПЫ РАЗВИТИЯ СТАНДАРТОВ БЕЗОПАСНОСТИ БЕСПРОВОДНОЙ СВЯЗИ СЕТИ G

БАРЩЕВСКИЙ Евгений Георгиевич
кандидат технических наук, профессор
ФГБОУ ВО «Государственный университет морского и речного флота им. адмирала С.О. Макарова»
г. Санкт-Петербург, Россия

В статье рассматриваются этапы развития стандартов безопасности беспроводной связи сети G. Дается характеристика каждого этапа развития, рассматриваются его преимущества и недостатки, определяются пути дальнейшего развития и совершенствования.
Ключевые слова: стандарты безопасности, беспроводная связь, этапы развития.

Введение (Introduction). Проблема безопасности в сотовых системах беспроводной связи возникла изначально для решения очень конкретной проблемы: как аутентифицировать пользователей, подключающихся к сети, и защищать соответствующие данные в пути от способных подслушивать радиоканал злоумышленников [1; 2]. Это всё должным образом было рассмотрено в нескольких поколениях сотовых систем. Были созданы технологии, которые постепенно достигли такого уровня защиты, что трудно найти какие-либо прорывные улучшения в этой области за последние годы [4].

Методы и материалы (Methods and Materials). В GSM (второе поколение) были реализованы аутентификация пользователя и шифрование на уровне радиоинтерфейса. Тем не менее, модель безопасности GSM оказалась крайне ненадежной. Криптографический алгоритм, принятый в аутентификации GSM (позже названный COMP-128) не был подтвержден криптографическим сообществом. Идея, которая впоследствии оказалась катастрофической, заключалась в том, что безопасность может быть обеспечена секретностью самого алгоритма. Этот алгоритм в частности, не обеспечивает взаимную аутентификацию.

Следующее третье поколение, UMTS, было поколением, в котором был достигнут наибольший прогресс в области безопасности. Во-первых, системы 3G полностью отказались от «безопасности через неясность», приняв публично проверенные криптографические алгоритмы семейства AES (*Advanced Encryption Standard*), которые намного безопаснее, чем предыдущие. Применение крип-

тографических методов также было значительно улучшено, как за счет явного разделения шифров и соответствующих ключей от целостности данных, так и за счет введения функций конфиденциальности и защиты пользователей от атак, отслеживающих положение конечного пользователя (конфиденциальность местоположения). Системы 3G также устранили проблему несанкционированных базовых станций, предоставив чрезвычайно эффективный метод взаимной аутентификации.

Примерно в 2011-2012 гг. началось распространение сетей стандарта 4G, который в настоящее время является текущим [5]. Этот стандарт стал, бесспорно, серьезным улучшением 3G, поскольку имеет такие преимущества, как улучшенная скорость загрузки и отправки данных, уменьшение задержек, практически кристалльно чистые голосовые звонки. Стандартный 4G (или 4G LTE) примерно в 5-7 раз быстрее, чем 3G, предлагая расчетно достижимые скорости до 150 Мбит/с. Это соответствует максимальной потенциальной скорости около 80 Мбит/с в реальном применении. К примеру, вы можете загрузить 2-х гигабайтный HD-фильм за 3 минуты 20 секунд в стандартной мобильной сети 4G, в то время как для сети 3G потребуется более 25 минут. Тем не менее, новая и даже более быстрая версия 4G уже доступна во многих странах под названием 4G LTE- Advanced (также известная как LTE-A, 4.5G или 4G+). Эта версия обеспечивает расчетные скорости до 1.5 Гбит/с.

Общая архитектура безопасности 4G была разделена на пять областей:

I. *Безопасность доступа к сети*: защита на уровне радиоинтерфейса и безопасный доступ пользователя к сервису.

II. *Безопасность сетевого домена:* защита сетевых элементов и соответствующего обмена трафиком данных и сигнальными сообщениями.

III**.** *Безопасность домена пользователя:* защита мобильного устройства и его взаимодействия с USIM.

IV. *Безопасность домена приложений:* безопасная связь на уровне приложений.

V. *Наглядность:* возможность проверить, работают ли (и какие) функции безопасности, а также как они настроены.

По оценкам GSMA в современном сетевом стандарте 5G есть потенциал, чтобы добавить ошеломляющие 2,2 триллиона долларов в мировую экономику в ближайшие 15 лет. Но приложения-убийцы, которые приносят доход и лояльность клиентов в эпоху 5G, будут сильно отличаться от того, что мы знаем сегодня. Бенефициарами 5G станут автономные транспортные средства, телездравоохранение, умные города и логистика – каждый из них на многомиллиардных рынках. Каждый из них также может подвергнуться значительным разрушениям, даже гибели людей, если их безопасность будет поставлена под угрозу. Для поддержки этих новых и интересных рыночных возможностей операторам необходим совершенно новый подход к управлению сетью, автоматизации и кибербезопасности. Для решения проблем, связанных с рисками 5G, сети будут полностью автоматизированы, а процессы, контролируемые программным обеспечением, станут неотъемлемой частью инфраструктуры 5G. Ручные процессы не будут соответствовать требованиям, скажем, развертывания автомобилей с автоматическим управлением в напряженный час пик. Следовательно, мантрой эпохи 5G будет «программируемость» или способность определять и контролировать каждый аспект сети в программном обеспечении, от ядра до края. Но эта программируемость является обоюдоострым мечом – она также дает хакерам средство вызывать хаос издалека. Важной основой при разработке безопасных систем является надежная архитектура для выявления угроз, а также для разработки и развертывания эффективных средств контроля безопасности. Это должно быть приоритетом первого дня, а не запоздалой мыслью. Чтобы это произошло эффективным образом, необходимо создать новую экосистему поставщиков, исследователей и операторов, которая будет управлять повесткой дня в области кибербезопасности для 5G. Эта архитектура должна предоставлять операторам гибкость в предоставлении услуг, которые требуются клиентам, в то же время отказывая злоумышленникам в любой возможности вызвать сбои. Интерфейсы прикладного программирования, также известные как API, которые обеспечивают программиру-

емость вместе с искусственным интеллектом (AI) и машинным обучением (ML), могут стать серебряными пулями поставщика услуг против кибератак.

Основное отличие сетей пятого поколения от 4G – скорость передачи данных: 20 Гбит/с против 1 Гбит/с при пиковых нагрузках. На практике пользователи 5G загружают файлы на скорости до 100 Мбит/с, тогда как у 4G этот показатель не превышает 10 Мбит/с. Например, в 5G серия фильма «Игра престолов» скачивается за одну минуту, а в сетях четвертого поколения – за 11 минут [3].

Среди других плюсов 5G – пониженное энергопотребление устройств, низкая задержка сигнала, более высокая пропускная способность и выход за пределы аппаратных решений: многие функции 5G реализованы программным способом, а не только на уровне физической инфраструктуры, как в сетях прошлых поколений.

Выводы (Summary). Новые стандарты беспроводной связи неизбежно ведут к цифровой трансформации. Помимо того, что сети и системы 5G значительно превосходят предыдущие поколения с точки зрения емкости и пропускной способности, они будут обеспечивать инфраструктуру для поддержки самых разных сервисов: промышленный Интернет вещей и интеллектуальные системы управления, автономные транспортные средства и дроны, жизненно важное электронное здравоохранение и удаленная хирургия, виртуальная и дополненная реальности, удаленная диагностика и профилактическое обслуживание и т. д. Число интернет-устройств стремительно растет, поэтому старые стандарты неизбежно приходится модернизировать. Чтобы нормально работать, многим устройствам необходима более высокая пропускная способность сети. 5G работает на других частотах, дает доступ в интернет большему количеству устройств, имеет сверхбыструю скорость и минимизирует задержки при передаче данных. Такие улучшения сети требуют радикально новый подход в модели безопасности, не похожий на используемый в сотовых системах до последнего четвертого поколения.

СПИСОК ЛИТЕРАТУРЫ

1. *Олейникова А.В., Нуртай М.Д., Шманов Н.М.* Перспективы развития связи 5G // Современные материалы, техника и технологии. – 2015. – №2(2). – С. 233-235
2. *Тихвинский В.О.* 5G WORLD SUMMIT– 2014: Курс прежний – ОТ 4G К 5G // T-Comm: Телекоммуникации и транспорт. – 2014. – Т. 8. № 7. – С. 95-96.
3. *Baracca A., Weber A., Wild T. and Grangeat C.* A statistical approach for RF exposure compliance boundary assessment in massive MIMO systems ‖ in Proceedings of the 22nd International ITG Workshop on Smart Antennas,WSA. PP. 1-6. Bochum. Germany. 2018.
4. *Tan W., Matthaiou M., Jin S. and Li X.* Spectral Efficiency of DFT-Based Processing Hybrid Architectures in Massive MIMO ‖ IEEE Wireless Communications Letters, 2017.
5. *Tan W., Xu G., De Carvalho E., Zhou M., Fan L. and Li C.* Low Cost and High Efficiency Hybrid Architecture Massive MIMO Systems Based on DFT Processing ‖ Wireless Communications and Mobile Computing. vol. 2018. PP. 1-11. 2018.

LITERATURE

1. *Oleinikova A.V., Nurtai M.D.,Shmanov N.M.* Prospects for the development of 5G communications // Modern materials, equipment and technologies. 2015. No. 2 (2). pp. 233-235.
2. *Tikhvinsky V.O.* 2355G WORLD SUMMIT – 2014: The course is the same - FROM 4G TO 5G // T-Comm: Telecommunications and transport. 2014. V. 8. No. 7. S. 95-96.
3. *Baracca A., Weber A., Wild T. and Grangeat C.* A statistical approach for RF exposure compliance boundary assessment in massive MIMO systems ‖ in Proceedings of the 22nd International ITG Workshop on Smart Antennas,WSA. PP. 1-6. Bochum. Germany. 2018.
4. *Tan W., Matthaiou M., Jin S. and Li X.* Spectral Efficiency of DFT-Based Processing Hybrid Architectures in Massive MIMO,‖ IEEE Wireless Communications Letters, 2017.
5. *Tan W., Xu G., De Carvalho E., Zhou M., Fan L. and Li C.* Low Cost and High Efficiency Hybrid Architecture Massive MIMO Systems Based on DFT Processing,‖ Wireless Communications and Mobile Computing. vol. 2018. PP. 1-11. 2018.

UDC 621.37К

STAGES IN THE DEVELOPMENT OF G WIRELESS SECURITY STANDARDS

BARSHCHEVSKY Evgeny Georgievich
Candidate in Technical Sciences, Professor
Admiral Makarov State University of Maritime and Inland Shipping
St. Peterburg, Russia

The article discusses the stages of development of wireless communication security standards of the G network. The characteristics of each stage of development are given, its advantages and disadvantages are considered, ways of further development and improvement are determined.
Key words: security standards, wireless communications, milestones.

АНАЛИЗ СТАТИСТИКИ ЛУЧШИХ ЗООПАРКОВ МИРА И РОССИИ

ВЕРХОГЛЯДОВА Александра Владимировна
магистрант
ФГБОУ ВО «Донской государственный технический университет»
г. Ростов-на-Дону, Россия

Лицо, собирающееся открыть зоопарк, вынуждено решать, какие виды ему стоит включать в список своего зоопарка, а какие придётся оставить без внимания. В этом деле он может опираться на опыт уже устоявшихся больших зоопарков, а может из своих личных приоритетов подобрать животных. При этом необходимо понимать разницу государственных и частных зоопарков, начальный капитал которых может сильно отличаться, так же, как и имеющаяся площадь.
Ключевые слова: математический анализ, статистика, зоопарк, анализ статистики, видовой состав, функции распределения.

Перед началом разработки математической модели видового состава городского зоопарка мы проводим дополнительные исследования, необходимые для корректного построения модели. Исследования основываются на анализе собранной статистики по лучшим зоопаркам мира. Полученные результаты станут обоснованием выбора параметров и ограничений для оптимизации, примером для сравнения полученных моделей, выявления преимуществ.

Для корректного исследования необходимо ознакомиться с реальными объектами, то есть провести сбор данных по зоопаркам на предмет видового состава кошачьих. Для этого была проведена выборка из сорока зоопарков (30 лучших зоопарков мира и 10 лучших зоопарков России) и построение таблицы по полученным данным. Выбор зоопарков осуществлялся из статей, которые на основе ряда параметров составляли топы лучших зоопарков мира, Европы и России. Демонстрация видового разнообразия находится в открытом доступе, на сайтах зоопарков.