Proceedings of the 16th International
Scientific and Practical Conference
«Challenges in Science of Nowadays»
(April 26-28, 2026).
Washington, USA

No
292

INFORMATION AND WEB TECHNOLOGIES

Современные угрозы безопасности дактилоскопических сенсоров: от физических муляжей до программных эксплойтов

Хайрулла Абилкайыр Абдуллаулы[1]

[1] студент II курса магистратуры;
Казахский национальный исследовательский технический университет имени К.И. Сатпаева; Республика Казахстан

Аннотация. В данной статье проводится комплексное исследование безопасности современных дактилоскопических систем аутентификации. Автор систематизирует технологические принципы работы емкостных, оптических и ультразвуковых сенсоров, выявляя их фундаментальные уязвимости. Особое внимание уделяется классификации угроз: от физического создания муляжей с помощью полимеров до программных эксплойтов на уровне доверенной среды исполнения (TEE). В работе анализируются современные методы защиты, включая алгоритмы распознавания «живого» объекта и криптографическую привязку компонентов.
Ключевые слова: *кибербезопасность, биометрическая аутентификация, Touch ID, защита данных, Liveness Detection.*

Введение. В современной экосистеме цифровой безопасности биометрическая аутентификация перешла из разряда футуристических технологий в стандарт де-факто для персональных и корпоративных устройств. Технологии дактилоскопического сканирования, широко известные под коммерческим названием Touch ID, занимают центральное место в этой парадигме. Благодаря идеальному балансу между удобством для пользователя (User Experience) и уровнем защищенности, отпечатки пальцев стали основным методом разблокировки смартфонов, подтверждения финансовых транзакций и доступа к критически важным инфраструктурам. Интеграция сенсоров непосредственно в экраны мобильных устройств и кнопки питания сделала биометрию невидимым, но мощным барьером на пути несанкционированного доступа.

Однако стремительное развитие технологий принесло не только новые методы защиты, но и принципиально иные векторы

угроз. Основная проблема заключается в том, что в отличие от паролей, биометрические данные неизменны: скомпрометированный отпечаток пальца нельзя «сбросить» или заменить. В последние годы наблюдается резкий рост доступности инструментов для обхода биометрических барьеров. Развитие высокоточной 3D-печати и появление специализированных полимерных материалов позволяют злоумышленникам создавать детализированные физические муляжи (Presentation Attacks) с минимальными затратами. Если раньше для создания качественного слепка требовались лабораторные условия, то сегодня «атака по отпечатку» может быть реализована с помощью бытовых химикатов и цифровой фотографии высокого разрешения.

Параллельно с физическими угрозами эволюционируют и программные эксплойты. Современные исследования показывают, что уязвимости могут скрываться не только в самом сенсоре, но и на пути передачи данных от датчика к процессору. Появление атак типа «Replay Attack», попытки внедрения в доверенную среду исполнения (TEE) и использование нейросетей для генерации «мастер-отпечатков» (MasterPrints) ставят под сомнение абсолютную надежность дактилоскопии. Таким образом, актуальность данного исследования обусловлена необходимостью систематизации современных угроз и критического анализа существующих методов защиты в условиях, когда инструменты взлома становятся доступнее, а методы атак – изощреннее.

1. Технологический базис: типы сенсоров и их физические принципы.

Понимание механизмов функционирования дактилоскопических сканеров является необходимым условием для анализа их защищенности. Физический принцип, лежащий в основе получения изображения отпечатка, определяет не только качество биометрического шаблона, но и те векторы атак, которым система будет наиболее подвержена. На сегодняшний день в потребительской электронике и системах контроля доступа доминируют три основные технологии: емкостная, оптическая и ультразвуковая.

Емкостные сенсоры: измерение разности потенциалов.

Емкостные сканеры являются наиболее распространенным типом датчиков, используемых в классических модулях Touch ID и кнопках питания смартфонов. Принцип их работы основан на использовании микроскопических конденсаторных пластин, интегрированных в чип сенсора. Когда палец прикладывается к поверхности, папиллярные линии (выступы) и впадины образуют обкладки конденсаторов вместе с электродами датчика.

Согласно законам электростатики, емкость конденсатора

INFORMATION AND WEB TECHNOLOGIES

обратно пропорциональна расстоянию между его обкладками. Выступы кожи, касающиеся защитного покрытия сенсора, создают высокую емкость, в то время как впадины, отделенные от датчика слоем воздуха (имеющим иную диэлектрическую проницаемость), создают значительно меньшую емкость. Встроенная интегральная схема (ASIC) преобразует эти изменения напряжения в цифровую карту. Ключевая особенность этой технологии заключается в том, что она требует наличия проводящего объекта, что в теории должно защищать от простых бумажных копий отпечатков, но делает систему уязвимой для токопроводящих полимерных муляжей.

Оптические сенсоры: сканирование изображения.

Оптические сенсоры – это старейшая технология, получившая «второе дыхание» с распространением OLED-дисплеев. В современных смартфонах такие датчики располагаются под экраном. Принцип их работы аналогичен цифровой камере: поверхность пальца освещается (через промежутки между пикселями дисплея), и отраженный свет фиксируется фоточувствительной матрицей (CMOS или CCD).

Алгоритм анализирует темные и светлые участки изображения, формируя 2D-картину папиллярного узора. Основным преимуществом является дешевизна и возможность подэкранного размещения. Однако с точки зрения безопасности 2D-оптическое сканирование является наиболее уязвимым. Поскольку сенсор «видит» лишь плоское изображение, он часто не способен отличить реальный объемный палец от высококачественной фотографии или распечатки, если в системе не реализованы дополнительные программные алгоритмы проверки «живости» (Liveness Detection). Более продвинутые оптические системы используют многоспектральное сканирование для анализа подповерхностных слоев кожи, что значительно усложняет задачу взлома.

Ультразвуковые сенсоры: акустическое построение рельефа.

Ультразвуковая технология представляет собой наиболее совершенный и защищенный на данный момент метод дактилоскопии. Работа датчика основана на принципе эхолокации: пьезоэлектрический передатчик испускает ультразвуковой импульс, который проходит через стекло экрана и отражается от поверхности пальца.

В отличие от оптических аналогов, ультразвук проникает в эпидермис, позволяя фиксировать не только поверхностный рисунок, но и глубинные детали, такие как поры и капилляры. Принимающее устройство измеряет время возврата эха и его интенсивность в каждой точке, формируя детализированную 3D-

модель отпечатка. Физика процесса такова, что ультразвук по-разному отражается от живой ткани, воздуха и искусственных материалов (силикона, пластика). Это делает технологию крайне устойчивой к физическим муляжам. Кроме того, такие сенсоры способны работать через загрязнения, влагу или жировую пленку, которые часто становятся препятствием для емкостных и оптических датчиков.

Таким образом, переход от простой фиксации изображения (оптика) к измерению электрических характеристик (емкость) и, наконец, к объемному акустическому сканированию (ультразвук) отражает эволюцию биометрических систем в сторону повышения их отказоустойчивости [1-2].

2. Классификация физических угроз (Presentation Attacks).

Атаки предъявления (Presentation Attacks, PA) представляют собой наиболее интуитивно понятный, но оттого не менее опасный класс угроз биометрическим системам. В международном стандарте ISO/IEC 30107 такие воздействия определяются как предъявление биометрическому сенсору артефакта или попытка имитации характеристик живого объекта для манипуляции результатом аутентификации. Успех физической атаки напрямую зависит от способности злоумышленника воспроизвести те физические свойства пальца, на которые ориентирован конкретный тип сканера.

Методология создания искусственных муляжей.

Процесс создания поддельного отпечатка (муляжа) прошел путь от сложных лабораторных манипуляций до использования бытовых материалов. В основе большинства методов лежит получение формы-матрицы. Это может быть реализовано либо контактным способом (например, использование стоматологической слепочной массы или воска), либо бесконтактным – путем цифровой обработки фотографии отпечатка, оставленного на стекле или металле, с последующей гравировкой или 3D-печатью формы.

После получения матрицы решающую роль играет выбор материала-заполнителя, который должен имитировать диэлектрические или оптические свойства кожи.

Полимерные материалы: силикон и желатин.

Силиконовые муляжи получили широкое распространение благодаря своей эластичности и способности с высокой точностью воспроизводить микрорельеф папиллярных линий. Силикон идеально подходит для обмана оптических сканеров, так как он эффективно рассеивает свет, имитируя визуальную текстуру человеческой ткани. Однако обычный силикон является диэлектриком, что делает его малоэффективным против емкостных

INFORMATION AND WEB TECHNOLOGIES

датчиков, которые требуют электропроводности.

Желатиновые составы (или «мармеладные» отпечатки) представляют собой еще более изощренную угрозу. Желатин по своим характеристикам близок к белковому составу человеческой кожи и обладает естественной влажностью. Это позволяет ему успешно обходить многие системы Liveness Detection, которые ориентированы на измерение влажности или специфического оптического поглощения. Более того, желатин обладает определенным уровнем электропроводности, что делает его опасным даже для емкостных сенсоров Touch ID.

Токопроводящие чернила и графитовые покрытия.

Для целенаправленного взлома емкостных сенсоров, которые измеряют разность потенциалов, злоумышленники используют специализированные составы. Ключевым вектором атаки здесь выступает добавление в полимерную основу токопроводящих чернил (на основе серебра или меди) или мелкодисперсного графитового порошка.

Принцип атаки заключается в создании муляжа, который не только повторяет рельеф, но и замыкает электрические цепи микроконденсаторов сенсора так же, как это делает живой палец. Современные методы включают струйную печать отпечатка на тонкой токопроводящей пленке. Такой «пластырь», наклеенный на палец злоумышленника, позволяет обмануть датчик, имитируя электрический отклик реального биологического объекта.

Атаки на основе 3D-печати и фотолитографии.

С развитием аддитивных технологий угроза перешла на новый уровень. Использование фотополимерных 3D-принтеров с высоким разрешением (до 10-25 микрон) позволяет восстановить объемную модель пальца по двухмерной фотографии. Злоумышленник может сфотографировать отпечаток пользователя на бокале или экране смартфона, повысить контрастность изображения в графическом редакторе и напечатать готовую накладку.

Такие методы особенно опасны для ультразвуковых сканеров. Если оптические и емкостные датчики можно обмануть плоской или полусферической подделкой, то ультразвук требует точного соблюдения глубины впадин и плотности материала. Использование композитных смол при 3D-печати позволяет добиться акустического импеданса, близкого к мягким тканям человека, что делает ультразвуковое сканирование уязвимым перед подготовленным атакующим.

Физические атаки эволюционируют в сторону гибридизации: современные муляжи сочетают в себе многослойные структуры, где один слой отвечает за рельеф (для оптики), а второй – за проводимость (для емкостных систем). Это ставит перед

разработчиками задачу внедрения более сложных методов Liveness Detection, способных анализировать глубокие биологические параметры, такие как пульсация капилляров или динамическое изменение давления, которые невозможно воспроизвести с помощью статического полимерного артефакта.

Атаки с использованием «мертвой зоны»: частичные и мастер-отпечатки.

Одной из наиболее критических уязвимостей современных дактилоскопических систем является их зависимость от частичных данных. В отличие от криминалистических сканеров, которые снимают полный отпечаток пальца «от края до края», миниатюрные сенсоры в мобильных устройствах имеют ограниченную площадь контакта. В результате система хранит в памяти не единое цельное изображение, а набор фрагментированных шаблонов (Minutiae), полученных в процессе регистрации пальца под разными углами.

Концепция «мертвой зоны» и частичных отпечатков. Когда пользователь прикладывает палец для аутентификации, сканер считывает лишь небольшую его часть (около 30-50%). Алгоритм сопоставления (Matcher) считает проверку успешной, если найден достаточный уровень совпадения между текущим фрагментом и любым из сохраненных шаблонов. Это создает «мертвую зону» безопасности: порог ложного принятия (False Acceptance Rate, FAR) намеренно занижается производителями для обеспечения удобства пользователя, чтобы ему не приходилось прикладывать палец с идеальной точностью.

Мастер-отпечатки (MasterPrints). На этой особенности базируется метод атак с использованием MasterPrints. Мастер-отпечатки – это синтетически созданные или отобранные из баз данных фрагменты папиллярных линий, которые обладают высокой степенью статистического сходства с большим количеством случайных отпечатков.

Исследования показывают, что человеческие отпечатки обладают определенными общими характеристиками в строении дуг и петель. Злоумышленники используют алгоритмы машинного обучения (в частности, GAN – Generative Adversarial Networks) для генерации «универсальных» шаблонов. Если в системе зарегистрировано несколько разных пальцев, вероятность того, что MasterPrint совпадет хотя бы с одним из фрагментов в базе, возрастает экспоненциально. Такая атака сопоставима с методом «перебора паролей» (Brute-Force), но вместо цифровых комбинаций используются специально спроектированные физические накладки или цифровые инъекции шаблонов.

Восстановление отпечатка по остаточному следу.

INFORMATION AND WEB TECHNOLOGIES

Латентные (скрытые) отпечатки пальцев представляют собой жировые и потовые следы, оставляемые пользователем на глянцевых поверхностях. В контексте биометрической безопасности наиболее опасны следы, оставленные непосредственно на стекле сканера или защитном покрытии экрана.

Уязвимость остаточного следа. Многие типы сенсоров, особенно оптические и некоторые емкостные, крайне чувствительны к физическому состоянию поверхности. Если пользователь успешно авторизовался и оставил четкий латентный след, злоумышленник может использовать его для повторного входа.

Существует несколько методов реактивации остаточного следа:

- ***Физическое воздействие:*** в некоторых случаях достаточно просто подышать на сенсор (увеличить влажность и температуру) и приложить мягкий материал (например, полиэтилен или подушечку пальца в перчатке), чтобы датчик снова считал существующий жировой след как реальный палец.
- ***Фотографирование и репликация:*** с помощью специального освещения и макросъемки латентный отпечаток на стекле смартфона может быть зафиксирован в высоком разрешении. Далее, используя методы, описанные в разделе 2, изображение подвергается цифровой обработке (инверсии и усилению контрастности) для создания физического муляжа.

Пылевые и графитовые методы. Классический криминалистический метод проявления отпечатков с помощью мелкодисперсного магнитного порошка или графита также применим для подготовки атак. Проявленный на самом устройстве отпечаток может быть «снят» с помощью липкой ленты и немедленно предъявлен сенсору. Проблема усугубляется тем, что современные олеофобные покрытия экранов со временем стираются, что способствует накоплению более четких и стабильных латентных следов.

Атаки на основе MasterPrints и латентных следов демонстрируют, что безопасность биометрии зависит не только от стойкости алгоритма шифрования, но и от математической вероятности совпадения узоров, а также от элементарной гигиены устройства [3-5].

3. Программные и аппаратные эксплойты (System-Level Attacks).

В то время как физические атаки направлены на обман первичного детектора (сенсора), атаки системного уровня

INFORMATION AND WEB TECHNOLOGIES

нацелены на внутренние логические интерфейсы и протоколы обмена данными. Основная уязвимость здесь кроется в том, что результат биометрического сканирования в конечном итоге преобразуется в электрический сигнал или цифровой пакет данных, который должен быть доставлен в «центр принятия решений» – защищенный процессор или анклав безопасности.

Атаки на канал передачи данных (Replay Attacks).

Атака повторного воспроизведения (Replay Attack) в контексте дактилоскопии заключается в перехвате валидного сигнала отпечатка пальца и его последующей имитации для несанкционированного доступа. В архитектуре мобильного устройства сенсор и основной процессор (SoC) физически разнесены и соединены через интерфейсы связи, такие как SPI (Serial Peripheral Interface) или I2C.

Механика перехвата сигнала. Если канал связи между контроллером сканера и защищенным хранилищем (например, Apple Secure Enclave или ARM TrustZone) не зашифрован должным образом, злоумышленник с помощью микрозондов или специализированного аппаратного сниффера может «прослушать» шину данных. В момент, когда легитимный пользователь прикладывает палец, атакующий записывает последовательность битов, соответствующую успешной авторизации. В дальнейшем, для получения доступа, злоумышленнику достаточно транслировать эту же последовательность непосредственно в порт процессора, имитируя работу сенсора. В этом случае система будет убеждена в присутствии живого пальца, даже если сам сканер в этот момент не активен.

Инъекция биометрических данных (Biometric Injection). Современным развитием Replay-атак является программная инъекция. В этом сценарии злоумышленник использует уязвимости на уровне ядра операционной системы или драйверов устройства. Вместо аппаратного подключения к шине используется вредоносное ПО, которое подменяет данные, поступающие от драйвера сканера в API аутентификации. Если операционная система доверяет входящему потоку данных без проверки их криптографической подписи и временной метки (Timestamp), вредоносный код может «скормить» системе заранее подготовленный цифровой шаблон легитимного отпечатка.

Проблема незащищенных интерфейсов в бюджетных сегментах.

Особую остроту проблема Replay-атак приобретает в устройствах среднего и бюджетного сегментов, где производители часто экономят на сквозном шифровании (End-to-End Encryption) между периферией и процессором. В таких архитектурах данные передаются в открытом виде. Более того,

INFORMATION AND WEB TECHNOLOGIES

использование унифицированных модулей сканеров позволяет злоумышленникам применять готовые эксплойты для массовых атак.

Методы противодействия на системном уровне.

Для защиты от подобных угроз современные системы используют концепцию Secure Match-on-Chip. В этой архитектуре процесс сопоставления отпечатка происходит непосредственно внутри микросхемы сенсора, и во внешний мир (к основному процессору) передается не изображение или шаблон, а только зашифрованный токен «Да/Нет».

Дополнительным эшелоном защиты выступает привязка конкретного экземпляра сенсора к конкретному процессору на этапе производства (Pairing). При попытке заменить сенсор на «шпионский» модуль или внедрить перехватчик в шину, криптографические ключи перестают совпадать, и система блокирует биометрический вход. Тем не менее, как показывает практика, наличие уязвимостей в прошивках контроллеров (Firmware) оставляет теоретическую возможность для обхода этих барьеров через низкоуровневые эксплойты.

Атаки на канал передачи данных доказывают, что безопасность Touch ID не заканчивается на поверхности стекла. Надежность системы зависит от целостности всей цепочки: от физического кремниевого кристалла сенсора до изолированных областей памяти процессора. Без надежного шифрования интерфейса SPI/I2C даже самый совершенный ультразвуковой сканер остается уязвимым перед аппаратным перехватом.

Уязвимости на уровне ОС и драйверов: обход проверок через внедрение вредоносного кода.

Безопасность систем Touch ID и их аналогов критически зависит от надежности программного посредника – драйвера и системных служб аутентификации. Несмотря на то, что современные операционные системы (iOS, Android) стремятся к максимальной изоляции биометрических процессов, архитектурные сложности и необходимость взаимодействия между различными уровнями ПО создают поверхность для атак.

Компрометация драйверов устройств. Драйвер дактилоскопического сенсора работает на уровне ядра (Kernel Level) или в привилегированном пространстве пользователя. Это делает его приоритетной целью для атакующих. Уязвимости типа «переполнение буфера» (Buffer Overflow) или «состояние гонки» (Race Condition) в коде драйвера могут позволить вредоносному ПО получить права суперпользователя (Root).

Как только злоумышленник получает контроль над драйвером, он может манипулировать логикой его работы. Например, вместо

INFORMATION AND WEB TECHNOLOGIES

реального процесса сканирования драйвер может принудительно возвращать операционной системе флаг SUCCESS (успех) при получении любого сигнала, даже если палец к сенсору не прикладывался. Такая подмена происходит на уровне системных вызовов, что делает атаку невидимой для пользователя.

Атаки на службы аутентификации (Biometric Framework Attacks). В операционных системах существует специализированный программный каркас (Framework), который управляет диалоговыми окнами биометрии и связью с приложениями. Вредоносный код, внедренный в системные процессы (например, через методы DLL Injection или Hooking), может перехватывать ответы от службы биометрии.

Одной из наиболее опасных техник является «перехват обратного вызова» (Callback Hooking). Когда приложение запрашивает проверку отпечатка, оно ожидает ответ от системного API. Внедренный код может модифицировать этот ответ «на лету». Таким образом, приложение получает подтверждение того, что отпечаток верен, хотя фактическая проверка в защищенной среде (TEE) могла даже не проводиться или завершиться ошибкой.

Уязвимости в реализации доверенной среды исполнения (TEE). Для защиты наиболее чувствительных операций современные процессоры используют Trusted Execution Environment – изолированную область, где выполняются операции сравнения шаблонов. Однако TEE не является абсолютно неприступной. История исследований в области кибербезопасности знает примеры эксплойтов, направленных на микропрограммы (Trustlets), работающие внутри TEE.

Если злоумышленнику удается эксплуатировать уязвимость в «доверенном» приложении, которое отвечает за хранение эталонных шаблонов отпечатков, он может:

- ***Инъекция шаблона:*** добавить отпечаток злоумышленника в базу доверенных шаблонов без ведома пользователя.
- ***Понижение уровня безопасности:*** программно отключить проверку «живости» (Liveness Detection), делая систему уязвимой для простейших муляжей, которые ранее блокировались на уровне софта.

Роль вредоносного ПО и «Screen Overlay» атак. В контексте ОС Android распространена атака типа «наложение экрана» (Screen Overlay). Хотя она напрямую не взламывает Touch ID, она обманом заставляет пользователя приложить палец к сенсору. Вредоносное приложение отрисовывает поверх системного окна свое изображение (например, фальшивое

уведомление или игру), скрывая реальный запрос на подтверждение крупной финансовой транзакции. Пользователь, думая, что разблокирует телефон, фактически подписывает перевод средств.

Программный уровень защиты Touch ID – это сложная многослойная структура, где слабость любого звена (от кода драйвера до логики системного API) нивелирует аппаратную стойкость сенсора. Программные эксплойты позволяют масштабировать атаки, делая их дистанционными. Это подчеркивает важность не только совершенствования датчиков, но и внедрения строгих политик верификации кода драйверов, использования механизмов аттестации системы и защиты от перехвата системных вызовов.

Атаки на доверенную среду исполнения (TEE/Secure Enclave).

Доверенная среда исполнения (Trusted Execution Environment, TEE) и ее аппаратная реализация в устройствах Apple – Secure Enclave Processor (SEP) – представляют собой изолированные подсистемы, работающие независимо от основной операционной системы. Именно здесь хранятся математические репрезентации (шаблоны) отпечатков пальцев и происходит их финальное сравнение. Однако, несмотря на высокий уровень изоляции, теоретические и практические исследования последних лет выявили ряд критических векторов атак на эти «цифровые сейфы».

Теоретические возможности извлечения шаблонов. Вопреки распространенному мнению, в TEE хранятся не изображения папиллярных линий, а зашифрованные хеш-суммы или векторы признаков. Теоретическая возможность извлечения этих данных базируется на атаках по побочным каналам (Side-Channel Attacks).

- ***Анализ энергопотребления (DPA):*** Измеряя микроколебания в потреблении энергии процессором в момент выполнения алгоритма сопоставления, злоумышленник может попытаться восстановить структуру обрабатываемого шаблона.
- ***Атаки по времени (Timing Attacks):*** Анализ задержек при выполнении криптографических операций в TEE может дать информацию о сложности или структуре хранимых биометрических данных.

Хотя извлечение «картинки» пальца практически невозможно, получение цифрового шаблона позволяет провести атаку типа «инверсия шаблона», воссоздав синтетический отпечаток, который будет иметь идентичный цифровой след.

INFORMATION AND WEB TECHNOLOGIES

Практические эксплойты: подмена результата аутентификации. На практике более реальной угрозой является не кража шаблона, а компрометация логики принятия решения внутри самой среды.

- ***Уязвимости микрокода (Firmware Vulnerabilities):*** в истории информационной безопасности известны случаи (например, эксплойты в архитектуре ARM TrustZone), когда ошибки в реализации монитора безопасного режима позволяли вредоносному коду из «незащищенного» мира (Normal World) проникать в память TEE. Получив доступ к памяти доверенного приложения, атакующий может выполнить операцию «патчинга» (Patching) в оперативной памяти, принудительно устанавливая флаг аутентификации в значение TRUE, независимо от того, какой палец был приложен к сенсору.
- ***Атаки на разделение памяти:*** в некоторых реализациях TEE разделяет кэш-память или другие аппаратные ресурсы с основным процессором. Использование уязвимостей типа Specter или Meltdown в контексте биометрии позволяет «подсматривать» за операциями внутри Secure Enclave, перехватывая промежуточные результаты вычислений.

Специфика Secure Enclave (Apple SEP). В архитектуре Apple Secure Enclave реализован механизм аппаратного шифрования, где ключи уникальны для каждого чипа и не могут быть считаны даже самой операционной системой. Однако практические атаки (например, Blackbird) продемонстрировали, что на старых моделях устройств возможно использование уязвимостей в загрузчике SEP. Это позволяет атакующему перехватить контроль над процессором безопасности до того, как он будет полностью изолирован, что теоретически открывает доступ к перебору паролей или манипуляции биометрическим статусом. Атаки на TEE и Secure Enclave являются вершиной мастерства в области эксплойтов. Они требуют глубоких знаний микроархитектуры процессоров и навыков низкоуровневой отладки [6-7].

4. Современные методы защиты.

Эволюция методов атаки заставляет разработчиков внедрять многоуровневые системы защиты, направленные не только на верификацию папиллярного узора, но и на подтверждение «живости» (Liveness) предъявляемого биометрического объекта. Современные контрмеры можно разделить на аппаратные, программные и архитектурно-криптографические.

Liveness Detection: аппаратные методы.

Аппаратные методы обнаружения атак предъявления (Presentation Attack Detection, PAD) базируются на интеграции

INFORMATION AND WEB TECHNOLOGIES

дополнительных сенсоров, которые анализируют физиологические параметры, практически невоспроизводимые в искусственных муляжах.

Фотоплетизмография (датчики пульса и кислорода): современные оптические и ультразвуковые сканеры могут быть дополнены источниками света разных длин волн. Гемоглобин в крови поглощает свет определенным образом, что позволяет датчику фиксировать пульсацию капилляров и уровень сатурации (SpO_2). Поскольку силиконовый или желатиновый муляж не обладает кровеносной системой, отсутствие динамического изменения светопоглощения мгновенно блокирует доступ.

Термометрия: датчики температуры проверяют, соответствует ли тепловой профиль объекта человеческому телу (36.6°C). Однако этот метод считается вспомогательным, так как муляж может быть предварительно нагрет атакующим.

Емкостный анализ проводимости: живая кожа обладает специфической диэлектрической проницаемостью и проводимостью из-за наличия пота и межклеточной жидкости. Аппаратные фильтры способны отличить электропроводность графитового муляжа от ионной проводимости живой ткани.

Liveness Detection: программные методы.

Программные методы (Software-based PAD) не требуют дополнительных датчиков и полагаются на интеллектуальную обработку данных, полученных со стандартного сканера.

Анализ микродинамики деформации: при нажатии живого пальца на сенсор кожа подвергается деформации: папиллярные линии слегка расширяются, а впадины сжимаются под давлением. Программные алгоритмы анализируют серию кадров в миллисекундном диапазоне. Искусственные материалы (даже эластичные) деформируются иначе, чем живая плоть, что позволяет нейросетевым моделям выявлять подделку.

Анализ пор и текстуры (Skin Pore Analysis): высокое разрешение современных сканеров позволяет идентифицировать микроскопические поры потовых желез. Их расположение уникально, а процесс их «схлопывания» и выделения влаги при контакте крайне сложно имитировать в полимерах.

Спектральный анализ изображения: использование алгоритмов машинного обучения для поиска микро-артефактов, характерных для муляжей (пузырьки воздуха в силиконе, следы 3D-печати или специфический шум матрицы при повторном сканировании фото-копии).

Криптографическая привязка сенсора.

Защита данных на пути от сенсора к процессору – критическое условие для предотвращения Replay-атак и

аппаратного перехвата.

Сквозное шифрование (End-to-End Encryption): современные протоколы (например, используемые в последних поколениях Touch ID) подразумевают, что данные зашифровываются непосредственно на кристалле сенсора с использованием ключа, сгенерированного в Secure Enclave. Таким образом, даже если злоумышленник подключится к шине SPI/I2C, он увидит только зашифрованный шум, расшифровка которого без доступа к аппаратному корню доверия (Root of Trust) практически невозможна.

Аппаратное сопряжение (Hardware Pairing): на этапе производства каждый сенсор получает уникальный идентификатор, который «привязывается» к центральному процессору. Эта цифровая подпись проверяется при каждой загрузке. Если система обнаруживает замену сенсора на неоригинальный (или на устройство-перехватчик), биометрические функции отключаются на аппаратном уровне.

Использование одноразовых меток (Nonces): чтобы предотвратить повторное воспроизведение ранее записанного сигнала, каждая сессия обмена данными снабжается случайным числом (Nonce) и временной меткой. Повторно отправленный пакет данных будет отклонен процессором как устаревший.

Современные методы защиты смещают акцент с анализа «картинки» на анализ «жизни». Комбинация мультиспектрального сканирования, анализа динамики нажатия и жесткой криптографической привязки компонентов делает современные системы Touch ID устойчивыми к большинству бытовых и коммерческих атак [8].

Заключение.

В данной работе был проведен комплексный анализ систем дактилоскопической аутентификации, охватывающий путь от физических основ функционирования сенсоров до высокоуровневых программных уязвимостей. Исследование показало, что, несмотря на доминирующее положение Touch ID в экосистеме мобильной безопасности, технологический базис каждого типа датчиков – от оптических до ультразвуковых – имеет свои фундаментальные ограничения, создающие специфические «окна возможностей» для реализации атак.

Классификация физических угроз (Presentation Attacks) демонстрирует, что доступность материалов для создания муляжей, таких как специализированные полимеры и токопроводящие чернила, нивелирует защищенность простых емкостных и оптических систем. В то же время анализ программных и аппаратных эксплойтов системного уровня

подчеркивает, что безопасность биометрии не ограничивается поверхностью сканера. Уязвимости в каналах передачи данных и доверенных средах исполнения (TEE) представляют собой наиболее опасный класс угроз, позволяющий обходить проверку без необходимости физического копирования отпечатка.

Современные методы защиты, рассмотренные в работе, показывают отчетливый тренд на интеллектуализацию биометрических систем. Внедрение многоуровневого распознавания «живого» объекта (Liveness Detection) и криптографическая привязка компонентов существенно усложняют задачу злоумышленника. Однако будущее этой области будет определяться противостоянием алгоритмов искусственного интеллекта. Появление угроз типа Deepmaster Prints, способных генерировать универсальные мастер-отпечатки с помощью нейросетей, требует от разработчиков симметричного ответа в виде адаптивных моделей защиты и перехода к мультимодальной аутентификации.

Подводя итог, можно утверждать, что биометрическая защита Touch ID остается надежным инструментом лишь при условии комплексного подхода, сочетающего физическую стойкость сенсора с архитектурной целостностью программного обеспечения. Результаты данного исследования могут быть использованы при проектировании защищенных систем доступа и в рамках дальнейшей разработки систем обнаружения вторжений на уровне конечных устройств.

References:

[1] Kosmos. (2022, November 3). Behind fingerprint biometrics: How it works and why it matters. https://www.1kosmos.com/resources/blog/behind-fingerprint-biometrics-how-it-works-and-why-it-matters
[2] andopen. (2023, June 28). Beyond the face: Understanding biometric presentation attacks and liveness detection. https://andopen.co.kr/beyond-the-face-understanding-biometric-presentation-attacks-and-liveness-detection/
[3] Aratek. (n.d.). The 4 fingerprint sensor types. https://www.aratek.co/news/the-4-fingerprint-sensor-types
[4] Fingerprint. (2024, March 14). How to harden your fingerprint implementation. https://fingerprint.com/blog/how-to-harden-your-fingerprint-implementation/
[5] Gonzalez-Soler, L. J., & Gomez-Barrero, M. (2023). Introduction to presentation attack detection in fingerprint biometrics. ResearchGate. https://www.researchgate.net/publication/368478557_Introduction_to_Presentation_Attack_Detection_in_Fingerprint_Biometrics
[6] Patel, V. V., & Mehta, S. (2018). Attacks on biometric systems: An overview. International Journal of Computer Science and Information

INFORMATION AND WEB TECHNOLOGIES

Security. https://www.researchgate.net/publication/322225967_Attacks_on_Biometric_Systems_An_Overview

[7] Smith, A., et al. (2025). DeepMasterPrints: Generative models for universal fingerprint creation. arXiv. https://arxiv.org/html/2504.11066v1 (Примечание: данные автора взяты на основе метаданных препринта 2025 года).

[8] Uludag, U., & Jain, A. K. (2004). Attacks on biometric systems: A case study in fingerprints. SPIE Defense and Security Symposium. https://biometrics.cse.msu.edu/Publications/SecureBiometrics/UludagJain_BiometricAttacks_SPIE04.pdf