Авторизация пользователей по QR-кодам, записанным с помощью импульсно-лазерной обработки материалов

М. В. Лобанок, С. С. Гринько, О. Р. Людчик

Белорусский государственный университет, Минск, Беларусь,
e-mail: LobanokMV@bsu.by

В работе рассматривается междисциплинарный подход к авторизации пользователей на рабочих местах с помощью физических QR-меток, записанных методом импульсной лазерной обработки в различных материалах, в качестве элемента системы контроля доступа. Обсуждаются сопротивляемость интегрированных меток несанкционированному копированию и физическому вмешательству, а также возможности интеграции предлагаемого решения в существующие системы кибербезопасности и управления доступом.

Ключевые слова: лазерная маркировка; QR-код; аутентификация; контроль доступа; физические метки.

User authorization using QR codes recorded using pulsed laser processing of materials

M. V. Lobanok, S. S. Grinko, O. R. Lyudchik

Belarusian Statel University, Minsk, Belarus, e-mail: LobanokMV@bsu.by

This paper examines an interdisciplinary approach to user authorization at workstations using physical QR tags embedded in various materials using pulsed laser processing as an element of an access control system. The resistance of integrated tags to unauthorized copying and physical interference, as well as the possibilities of integrating the proposed solution into existing cybersecurity and access control systems, are discussed.

Keywords: Distance education; information and communication technologies; academic integrity.

Введение

Современные рабочие процессы предъявляют высокие требования к надежности систем управления доступом и аутентификации. В промышленных и корпоративных средах широко применяются физические идентификаторы личности – электронные пропуска, RFID-метки, смарт-карты, биометрия – для получения сотрудниками доступа к оборудованию или данным. Однако традиционные методы подвержены ряду уязвимостей: карты и метки могут быть утеряны или скопированы, пароли – перехвачены злоумышленниками. Поэтому актуальной задачей является объединение кибербезопасности с физическими факторами непосредственно на рабочем месте, что затрудняет удаленные атаки и подмену устройств.

Одним из перспективных решений является использование QR-кодов, интегрированных в оборудование, в качестве меток для авторизации. QR-коды получили широкое распространение как удобный носитель машиночитаемой информации; они применяются для маркировки изделий и отслеживания компонентов по цепочкам поставок. Однако стандартный статический QR-код сам по себе не

обеспечивает криптографической стойкости: будучи открытым идентификатором, такой код может быть сравнительно легко скопирован или подменен злоумышленником. Известны случаи, когда на объектах злоумышленники наклеивали поверх настоящих QR-стикеров поддельные, перенаправляя пользователей на мошеннические ресурсы. В итоге обычный распечатанный QR-код годится скорее для упрощения доступа к информации, чем для надежной аутентификации.

В данной работе предлагается подход, повышающий доверие к QR-меткам путем записи QR-кода в материал с помощью лазерной гравировки. Импульсная лазерная маркировка позволяет нанести на металл, пластик или другой материал стойкое изображение с высокой точностью и контрастом. Такие метки не выцветают, не стираются со временем, не боятся влаги и химического воздействия; попытка незаметно удалить или заменить их существенно затруднена. Важно, что присутствие физической метки привязывает пользователя к конкретному оборудованию в момент доступа, дополняя его учетные данные и повышая защиту от удаленного взлома.

Цель данного исследования – комплексно изучить возможности и ограничения использования лазерно-гравированных QR-меток для авторизации пользователей на рабочих местах.

Протокол авторизации с физической QR-меткой

Предлагаемый способ аутентификации сочетает сканирование физического QR-кода, нанесенного на оборудование, с проверкой цифровых учетных данных пользователя через защищенный канал. Каждый защищаемый объект (рабочая станция, терминал, станок и т. п.) имеет уникальный QR-код, лазерно выгравированный на корпусе или панели. Этот код может содержать идентификатор устройства либо зашифрованный URL для обращения к серверу аутентификации. Процедура авторизации включает несколько этапов. Во-первых, пользователь инициирует вход в систему на рабочем месте (например, пытается войти в учетную запись компьютера или запустить станок); система запрашивает подтверждение присутствия пользователя у данного устройства. Далее пользователь с помощью доверенного мобильного устройства (смартфона с корпоративным приложением) либо со встроенного стационарного считывателя сканирует QR-метку на оборудовании. Примером аналогичного подхода в промышленности является система компании Sumitomo, где оператор идентифицируется сканированием QR-кода на своем бейдже, содержащем его имя и уровень доступа. После считывания метки приложение расшифровывает данные QR-кода и передает на сервер (по защищенному протоколу TLS) следующую информацию: (a) идентификатор устройства, зашифрованный или закодированный в метке; (b) учетные данные пользователя (например, токен сеанса приложения или его электронную подпись). Сервер сопоставляет полученные данные с базой доступа: пользователь считается подлинным и получает разрешение, только если его электронные креденшелы валидны и он предъявил правильную метку от данного устройства. Физическое сканирование таким образом привязывает сессию к конкретному месту и выступает фактором присутствия. Требование иметь при себе доверенный сканер (смартфон с приложе-

нием) добавляет дополнительный out-of-band уровень безопасности сверх обычного пароля. При успешной проверке система предоставляет доступ (разблокирует ПК, запускает оборудование и т. д.) и регистрирует событие в жур-нале безопасности. Заметим, что сам QR-код в данной схеме не содержит чувствительных данных (например, паролей); он служит лишь меткой-связкой между физическим объектом и записью в системе доступа. Без знания учетных данных пользователя сканирование даже настоящего кода не позволит злоумышленнику пройти аутентификацию.

Следует учитывать, что простая передача статичного идентификатора сопряжена с риском атаки воспроизведения (replay): противник теоретически может скопировать QR-код и попытаться использовать его на поддельном устройстве. Для повышения стойкости возможны усовершенствования протокола за счет внедрения динамических компонентов. В частности, реализуемо комбинированное решение, когда после ввода пароля система генерирует одноразовый challenge, который либо отображается на экране в виде временного QR-кода, либо обрабатывается на мобильном клиенте. Однако в нашем исследовании основное внимание уделено статической физической метке как фактору присутствия, в сочетании с проверкой пользователя через доверенное приложение. Такой подход уже обеспечивает двухфакторную авторизацию (знание пароля + обладание смартфоном для сканирования in situ), а также препятствует удаленной компрометации, требуя непосредственного нахождения у защищаемого устройства.

Для создания стойких QR-меток применяется технология импульсной лазерной обработки. Режим наносекундных импульсов позволяет локально воздействовать на поверхность – испаряя или оплавляя тонкий поверхностный слой – без существенного нагрева окружающей области. В результате на материале формируются контрастные элементы QR-кода заданной формы (темные или светлые относительно фона), которые считываются оптическими сканерами. Лазер выполняет гравировку или микромодификацию поверхности (окисление, оплавление, вспенивание полимера и т. п.), оставляя неизгладимую метку с размером элементов порядка десятков–сотен микрометров.

Считывание полученных QR-меток осуществлялось с помощью камеры смартфона (12 Мп) через мобильное приложение-сканер (на основе библиотеки ZXing), а также ручным 2D-сканером штрихкодов для сравнения. В штатных условиях (прямой угол обзора ~0°, расстояние ~20 см, освещение ~500 лк) все протестированные метки распознавались мгновенно, без ошибок декодирования. Среднее время считывания составляло менее 0,5 с. Для каждой метки было проведено не менее 50 попыток сканирования; во всех случаях результат был успешным, что свидетельствует о 100 % распознаваемости при отсутствии повреждений.

Далее метки подвергались испытаниям в усложненных условиях, чтобы оценить границы их работоспособности. Во-первых, проверялась устойчивость к изменению угла обзора и дистанции. Коды оставались уверенно читаемыми при наклоне до ~50° от перпендикуляра и при удалении до 1 м (при перефокусировке камеры). При более острых углах (> 60°) для металлических образцов наблюдались бликовые засветы, затруднявшие распознавание; проблему удавалось решить

использованием поляризационного фильтра на подсветке либо повторным сканированием под несколько иным углом. Во-вторых, оценивалось влияние частичного закрытия или повреждения метки. Имитируя загрязнение или износ, часть площади каждого QR-кода (от ~5 % до 30 %) закрашивалась непрозрачной краской. Эксперименты подтвердили, что при закрытии до ~15 % области (что соответствует запасу коррекции уровня M) все метки продолжали правильно декодироваться. При потере 20–30 % модулей вероятность успешного считывания зависела от расположения дефектов: если затерянные элементы были разбросаны, код зачастую удавалось восстановить за счет избыточности, тогда как выпадение нескольких соседних символов приводило к ошибкам декодера. Для уровня коррекции H (до 30 % восстановления) ожидаемо наблюдалась большая толерантность к повреждениям, хотя при этом сама плотность размещения модулей выше, что предъявляет более строгие требования к разрешающей способности сканирования.

Для противодействия угрозе копирования предлагается несколько подходов. Во-первых, можно усложнить воспроизведение метки добавлением скрытых элементов защиты. В промышленности существуют решения, интегрирующие в рисунок QR-кода микроструктуры или микроперфорацию по секретному шаблону. Такие элементы невидимы невооруженным глазом и не влияют на считывание основного кода, но могут быть обнаружены специальным прибором или приложением; их невозможно точно скопировать без знания шаблона, что значительно повышает барьер для подделки. Аналогично вокруг или внутри лазерного QR-кода можно нанести микротекст, голографические отметки либо использовать свойства материала (например, особое лазерное травление, видимое только под ультрафиолетом). Перспективным направлением является применение физически неклонируемых функций (PUF) – уникальных микродефектов и случайных структур поверхности, которые неизбежно возникают при лазерной обработке. Каждая такая метка будет обладать индивидуальным «отпечатком» на микроскопическом уровне, по которому можно подтвердить ее подлинность, и который чрезвычайно трудно подделать в принципе.

Во-вторых, важна система мониторинга и аудита использования меток. Поскольку при нашем подходе сканирование метки связано с сетевым сервером, несложно отслеживать время и место каждого обращения. Если один и тот же идентификатор QR внезапно будет сканироваться почти одновременно в двух разных локациях, система сможет заподозрить дублирование (клонирование метки) и принять меры – например, временно заблокировать доступ до разбирательства. Подобный подход успешно применяется для обнаружения клонированных карт доступа RFID и может быть адаптирован для QR-меток. Кроме того, ведение журнала всех попыток доступа повышает общую безопасность: администраторы впоследствии могут проверить, кто, когда и к какому оборудованию получал доступ, и выявить аномалии или нарушения регламента.

С точки зрения интеграции в существующую инфраструктуру кибербезопасности, предложенное решение достаточно гибко. Физические QR-метки могут использоваться как один из факторов многофакторной аутентификации.

Сканирование QR-кода на рабочем месте можно рассматривать как аналог подключения аппаратного токена: это требование, выполняемое пользователем (приложением на его устройстве) отдельно от основной системы. Большинство современных платформ управления доступом (IAM) позволяют добавить такой шаг проверки без значительных модификаций. Например, корпоративную систему входа можно настроить так, что при попытке войти в учетную запись с нового компьютера или терминала пользователь должен отсканировать соответствующий QR-код через приложение – и только после этого ему выдается токен сеанса. Такой принцип совместим со стандартными протоколами (OAuth 2.0, SAML и др.), где мобильное приложение выступает поставщиком аутентификации.

Разумеется, лазерно-гравированные QR-метки не являются панацеей и имеют границы применимости. В крайне агрессивных условиях эксплуатации (например, при постоянном абразивном износе, сильной коррозии или механических повреждениях) со временем метки могут деградировать. Кроме того, остаются актуальными общие проблемы информационной безопасности: атаки инсайдеров и методы социальной инженерии. Пользователи должны осознавать важность защиты своих учетных данных и не допускать раскрытия или несанкционированного использования доверенных устройств для сканирования. При соблюдении этих мер предложенная технология способна органично дополнить существующие средства кибербезопасности, добавляя новый уровень защиты на стыке цифрового и физического пространства.

Представлен комплексный подход к повышению безопасности авторизации пользователей на рабочих местах за счет физической интеграции QR-кода методом лазерной гравировки. Показано, что такие лазерно-гравированные QR-метки могут успешно выполнять роль дополнительного фактора аутентификации, обладая высокой надежностью считывания и устойчивостью к внешним воздействиям.

Библиографические ссылки

1. *Kamalanathan D.* Laser Engraved 2D and QR Code on Titanium Plates Denture Markers – An Observational Study / D. Kamalanathan, N. R. Monica, R. Sridharan // Journal of Research in Medical and Dental Science. 2022. Vol. 10, No 4. P. 70–73.
2. *Людчик О. Р., Лобанок М. В.* Влияние параметров лазерной обработки на характеристики рассеивающих массивов дефектов в стекле // Взаимодействие излучений с твердым телом: материалы XV Междунар. конф., Минск, 26–29 сентября 2023 г. – Минск: БГУ, 2023. С. 267–269.
3. Реализация учебного комплекса для измерения характеристик массивов лазерных пробоев в стекле / С. С. Гринько [и др.] // Компьютерные технологии и анализ данных (CTDA’2024): материалы IV Междунар. конф., Минск, 25–26 апреля 2024 г. – Минск: БГУ, 2024. С. 56–58.
4. Электрофизические характеристики структур TiAlCN/TiAlN, модифицированных наносекундной импульсной лазерной обработкой / О. С. Сиренко [и др.] // Квантовая электроника: материалы XIV Междунар. науч.-техн. конф., Минск, 21–23 ноября 2023 г. – Минск: БГУ, 2023. С. 453–456.