



استخدام مكتبة ZXING لزيادة أمان رمز الاستجابة السريعة

Баяманова Айжамал
Студентка, Белорусский
национальный
технический
университет

أيزهامل بايامانوف
طالبة في الجامعة التقنية
الوطنية البيلاروسية

Аннотация: В данной работе рассматриваются современные угрозы безопасности, связанные с использованием QR-кодов, и предлагается библиотека ZXing в качестве универсального решения для их защиты. Обсуждаются методы применения криптографических подписей и интеграции с блокчейн-технологиями для предотвращения подделки и фишинга. Библиотека ZXing выделяется как мощный и мультиплатформенный инструмент, способствующий улучшению процессов идентификации и аутентификации.

Ключевые слова: *Защита данных, QR-коды, безопасность, аутентификация, идентификация.*

الخلاصة : تبحث هذه الورقة البحثية في التهديدات الأمنية الحديثة المرتبطة باستخدام رموز الاستجابة السريعة (QR code) وتقدم مكتبة ZXing كحل عالمي لحمايتها. وتناقش طرق استخدام التوقيعات التشفيرية والتكامل مع تقنيات blockchain لمنع التزوير والنصيد. تتميز مكتبة ZXing بأنها أداة قوية ومتعددة المنصات تساعد على تحسين عمليات التعريف والمصادقة.

الكلمات المفتاحية : حماية البيانات، رموز الاستجابة السريعة، الأمان، المصادقة، التعريف.

**научный
руководитель**



Ковалева Ирина Львовна
к.т.н., доцент кафедры
«Программное обеспечение
информационных систем и
технологий» БНТУ

د. ايرينا ليفينا كوفاليفا
أستاذ مشارك في قسم برمجيات نظم
المعلومات والتكنولوجيا بالجامعة التقنية
الوطنية البيلاروسية

Введение

Работа направлена на исследование проблем безопасности QR-кодов и поиск решений для предотвращения угроз подделки и фишинга. Актуальность темы определяется широким использованием QR-кодов в системах идентификации и рисками их компрометации. В качестве эффективного инструмента предлагается библиотека ZXing, обеспечивающая надежную защиту благодаря криптографическим методам и возможностям интеграции с современными технологиями [1-4].

Результаты и обсуждение

QR-коды (Quick Response codes) стали важным инструментом для идентификации и аутентификации благодаря своей простоте, универсальности и высокой скорости обработки данных. Они широко используются в различных сферах, включая финансовые услуги, маркетинг и логистику. Тем не менее, их популярность привела к возникновению новых угроз, связанных с безопасностью. Основными рисками при использовании QR-кодов являются подделка и фишинг, что может привести к серьезным последствиям для пользователей.

Одним из наиболее распространённых сценариев угрозы является атака на пользователей банковских приложений. В этом случае злоумышленники могут заменить легитимный QR-код на поддельный, перенаправляя пользователей на фишинговые сайты, которые имитируют интерфейсы онлайн-банкинга. Такие сайты часто выглядят совершенно идентично оригинальным, что затрудняет пользователям выявление мошенничества. В результате пользователи вводят свои личные данные, такие как логины и пароли, что открывает доступ к их банковским счетам. Этот сценарий подчеркивает необходимость разработки эффективных методов защиты QR-кодов.

Для предотвращения угроз подделки и фишинга предлагается использовать open-source библиотеку ZXing. Эта библиотека выделяется своей мультиплатформенностью, поддерживая интеграцию с Android, iOS и веб-приложениями. Такой подход делает ZXing универсальным инструментом для работы с QR-кодами и позволяет разработчикам внедрять его в различные системы с минимальными усилиями.

Одним из ключевых направлений использования ZXing является интеграция с системами проверки подлинности данных. В частности, предлагается применение криптографических подписей для генерации QR-кодов. QR-коды, сгенерированные на основе криптографических подписей, могут быть проверены на этапе декодирования. Это позволит удостовериться в их подлинности и предотвратит случаи подделки. Криптографические подписи обеспечивают высокий уровень защиты, так как любые изменения в коде ведут к нарушению целостности подписи, что делает подделку QR-кода практически невозможной.

Кроме того, интеграция ZXing с блокчейн-технологиями открывает новые горизонты для повышения безопасности QR-кодов. Блокчейн, как распределённый реестр, обеспечивает прозрачность и защищённость данных. Запись информации о QR-коде в блокчейн позволяет отслеживать его происхождение и использование, что делает невозможной подмену кода без согласования с системой. Это свойство блокчейна потенциально может кардинально изменить методы аутентификации, предоставляя пользователям уверенность в том, что они взаимодействуют с легитимными ресурсами.

Важно отметить, что реализация предложенных решений требует комплексного подхода, включающего не только технические аспекты, но и обучение пользователей. Образовательные программы, направленные на повышение осведомленности о рисках, связанных с использованием QR-кодов, могут значительно снизить вероятность успешных атак. Пользователи должны быть информированы о том, как распознавать поддельные QR-коды и какие меры предосторожности следует применять при их сканировании.

Заключение

QR-коды остаются важным инструментом для идентификации и аутентификации, но их безопасность требует внимания. Использование библиотеки ZXing в сочетании с криптографическими подписями и блокчейн-технологиями может значительно повысить уровень защиты от подделки и фишинга. Однако успех этих мер зависит от комплексного подхода, включающего как технологические решения, так и повышение осведомленности пользователей о потенциальных угрозах. Только совместными усилиями можно создать безопасную среду для использования QR-кодов в различных сферах.

المقدمة

يهدف العمل إلى دراسة القضايا الأمنية المتعلقة برموز الاستجابة السريعة (QR Codes) وإيجاد حلول لمنع التهديدات المقلدة والتصيد الاحتيالي. وتحدد أهمية الموضوع من خلال الاستخدام الواسع النطاق لرموز الاستجابة السريعة (QR Codes) في أنظمة التعريف ومخاطر اختراقها. تم اقتراح مكتبة ZXing كأداة فعالة توفر حماية موثوقة بفضل أساليب التشفير والقدرة على التكامل مع التقنيات الحديثة [4-1].

النتائج والمناقشة

أصبحت رموز الاستجابة السريعة (QR Codes) أداة مهمة للتعريف والمصادقة بسبب بساطتها وتنوعها وسرعتها العالية في معالجة البيانات. يتم استخدامها على نطاق واسع في مختلف المجالات بما في ذلك الخدمات المالية والتسويق والخدمات اللوجستية. ومع ذلك، فقد أدت شعبيتها إلى ظهور تهديدات أمنية جديدة. المخاطر الرئيسية عند استخدام رموز الاستجابة السريعة (QR Codes) هي التزوير والتصيد الاحتيالي، مما قد يؤدي إلى عواقب وخيمة على المستخدمين.

أحد أكثر سيناريوهات التهديد شيوعاً هو الهجوم على مستخدمي تطبيقات الخدمات المصرفية. في هذه الحالة، يمكن للمهاجمين استبدال رمز الاستجابة السريعة الشرعي بآخر مزيف، وإعادة توجيه المستخدمين إلى مواقع التصيد الاحتيالي التي تحاكي واجهات الخدمات المصرفية عبر الإنترنت. غالباً ما تبدو مثل هذه المواقع متطابقة تماماً مع المواقع الأصلية، مما يجعل من الصعب على المستخدمين اكتشاف الاحتيال. نتيجة لذلك، يقوم المستخدمون بإدخال بياناتهم الشخصية، مثل معلومات تسجيل الدخول وكلمات المرور، مما يفتح إمكانية الوصول إلى حساباتهم المصرفية. يسلط هذا السيناريو الضوء على الحاجة إلى تطوير أساليب فعالة لحماية رموز الاستجابة السريعة (QR).

لمنع تهديدات التزوير والتصيد الاحتيالي، يُقترح استخدام مكتبة ZXing مفتوحة المصدر. تتميز هذه المكتبة بطبيعتها متعددة المنصات، حيث تدعم التكامل مع تطبيقات Android و iOS والويب. يجعل هذا النهج من ZXing أداة عالمية للعمل مع رموز QR ويسمح للمطورين بتنفيذها في أنظمة مختلفة بأقل جهد.

أحد المجالات الرئيسية لاستخدام ZXing هو التكامل مع أنظمة مصادقة البيانات. وعلى وجه الخصوص، من المقترح استخدام التوقيعات التشفيرية لتوليد رموز الاستجابة السريعة (QR). يمكن التحقق من رموز QR التي تم إنشاؤها بناءً على التوقيعات التشفيرية في مرحلة فك التشفير. وهذا من شأنه ضمان صحتها ومنع حالات التزوير. توفر التوقيعات التشفيرية مستوى عاليًا من الحماية، حيث أن أي تغييرات في الكود تؤدي إلى انتهاك سلامة التوقيع، مما يجعل تزوير رمز الاستجابة السريعة مستحيلًا تقريبًا.

علاوة على ذلك، فإن تكامل ZXing مع تقنية blockchain يفتح أفقاً جديدة لتعزيز أمن رمز الاستجابة السريعة. تضمن تقنية البلوكشين، باعتبارها سجلاً موزعاً، الشفافية وأمان البيانات. يسمح تسجيل المعلومات حول رمز الاستجابة السريعة (QR Code) في blockchain بمتابعة مصدره واستخدامه، مما يجعل من المستحيل استبدال الرمز دون موافقة من النظام. تتمتع هذه الخاصية في blockchain بالقدرة على إحداث ثورة في طرق المصادقة، مما يمنح المستخدمين الثقة في أنهم يتفاعلون مع موارد مشروعة.

ومن المهم ملاحظة أن تنفيذ الحلول المقترحة يتطلب نهجًا شاملاً، لا يشمل الجوانب الفنية فحسب، بل يشمل أيضًا تدريب المستخدم. يمكن للبرامج التعليمية التي تهدف إلى رفع مستوى الوعي بالمخاطر المرتبطة باستخدام رموز الاستجابة السريعة (QR Codes) أن تقلل بشكل كبير من احتمال وقوع هجمات ناجحة. يجب إعلام المستخدمين بكيفية التعرف على رموز الاستجابة السريعة المزيفة وما هي الاحتياطات التي يجب اتخاذها عند مسحها ضوئيًا.

الخاتمة

تظل رموز الاستجابة السريعة (QR Codes) أداة مهمة للتعريف والمصادقة، ولكن أمانها يتطلب الاهتمام. إن استخدام مكتبة ZXing مع التوقيعات التشفيرية وتقنيات blockchain يمكن أن يزيد بشكل كبير من مستوى الحماية ضد التزوير والتصيد الاحتيالي. ومع ذلك، فإن نجاح هذه التدابير يعتمد على اتباع نهج شامل يتضمن الحلول التكنولوجية وتوعية المستخدمين بالتهديدات المحتملة. من خلال الجهود المشتركة فقط يمكننا خلق بيئة آمنة لاستخدام رموز الاستجابة السريعة في مختلف المجالات.

المراجع والمصادر Literature

1. ZXing Team. ZXing: Open-Source Barcode Image Generation and Processing // GitHub 2024 [Электронный ресурс] – Режим доступа: <https://github.com/zxing/zxing>.
2. Wang, Y., & Li, X. The Role of QR Codes in Digital Transformation: Security and Authentication // Journal of Digital Technology. 2021. – P. 45-62.
3. Kumar, P., & Gupta, S. QR Code-Based Two-Factor Authentication Systems // International Journal of Information Security. 2023. – P. 123-134.
4. Носов А.А. Генерация QR-кодов // Электронная библиотека УрГПУ. [Электронный ресурс] – Режим доступа: <http://elar.uspu.ru/bitstream/uspu/3088/1/03Nosov2.pdf>

