QsecR- A Secure and Privacy-friendly Android QR code Scanner According to a Malicious URL Detection Framework

ABSTRACT Malicious Uniform Resource Locators (URLs) are the major issue posed by cybersecurity threats. Cyberattackers spread malicious URLs to carry out attacks such as phishing and malware, which lead unsuspecting visitors into scams, resulting in monetary loss and information theft. The adoption of Quick Response (QR) codes with malicious URLs is a growing concern and an open security issue. The existing QR link detection scanner applications mostly utilize the blacklist method to detect malicious URLs, which is not the optimal method for detecting new websites. Recently, machine learning methods have gained popularity as a means of enhancing the detection of malicious URLs. However, these methods are entirely data-dependent, and a large and updated dataset is required for the training to create an effective detection method. This research proposes QsecR, a secure and privacy-friendly QR code scanner, according to a heuristic malicious URL detection framework. QsecR is an Android QR code scanner based on predefined static feature classification by employing 39 classes of blacklist, lexical, host-based, and content-based features. A dataset containing 2000 real-world random URLs was gathered from URLhaus and PhishTank. The QsecR is evaluated by several QR code scanners in terms of security and privacy. The experimental result shows that QsecR outperforms others and achieves a detection accuracy of 94.65% and a precision value of 95.80%, which are significantly higher than the current secure QR code scanners. Also, QsecR is the most privacy-friendly application with the least privilege permission.

INDEX TERMS Android security, malicious URL detection, privacy-friendly application, QR code scanner, QR code security