STM JOURNALS

Journal of
Network Security

ISSN: 2395-6739 (Online)
ISSN: 2321-8517 (Print)
Volume 12, Issue 2, 2024
May–August
DOI (Journal): 10.37591/JoNS

https://journals.stmjournals.com/jons

Research JoNS

Cracking the Code: A Study on Exploitable Weaknesses in QR Code Technology

Aiswarya Dwarampudi[1,*], Yamuna Mundru[2], Manas Kumar Yogi[3]

Abstract

This study investigates the exploitable weaknesses inherent in quick response (QR) code technology, aiming to provide insights into potential security risks and mitigation strategies. QR codes, ubiquitous in modern society, serve various purposes ranging from marketing to authentication. However, their widespread utilization also renders them vulnerable to exploits by malicious actors. The research identifies common vulnerabilities such as data tampering, code injection, and phishing attacks, which can have significant consequences, including financial losses, data breaches, and privacy violations. To address these vulnerabilities, the study proposes a multifaceted approach encompassing authentication mechanisms, secure QR code generation practices, and user awareness programs. Furthermore, emphasizing compliance with industry standards and regulations is highlighted as a crucial aspect of QR code security. Through a comprehensive analysis of QR code weaknesses and their implications, this study underscores the importance of proactively addressing security risks to maintain trust and integrity in digital transactions involving QR codes. By enhancing QR code security measures and fostering collaboration among stakeholders, organizations and individuals can mitigate risks and ensure the reliability of QR code–based interactions in an increasingly interconnected digital landscape.

Keywords: Quick response (QR) code, pattern, security, data protection, encoding, decoding

INTRODUCTION

Overview of QR Code Technology

Quick response (QR) codes are now deeply ingrained in our everyday routines, spanning across multiple industries with their adaptable uses [1, 2]. These two-dimensional barcodes, originally developed in Japan, have gained widespread adoption globally due to their efficiency in storing and transmitting data. Unlike conventional barcodes, QR codes have the capacity to store a diverse array of data such as URLs, text, contact information, and product details, rendering them indispensable assets for both businesses and consumers. Across diverse industries such as marketing, retail, healthcare, transportation, and authentication, QR codes serve as efficient conduits for data exchange and interaction, facilitating tasks such as product tracking, mobile payments, patient identification, ticketing, and authentication processes.

***Author for Correspondence**
Aiswarya Dwarampudi
E-mail: aiswarya.d@pragati.ac.in

[1]Assistant Professor, CSE Department, Pragati Engineering College, Near Kakinada, Kakinada District, Andhra Pradesh, India
[2]Assistant Professor, CSE –AI & ML Department, Pragati Engineering College, Near Kakinada, Kakinada District, Andhra Pradesh, India
[3]Assistant Professor, CSE Department, Pragati Engineering College, Near Kakinada, Kakinada District, Andhra Pradesh, India

Received Date: February 29, 2024
Accepted Date: April 25, 2024
Published Date: July 02, 2024

Citation: Aiswarya Dwarampudi, Yamuna Mundru, Manas Kumar Yogi. Cracking the Code: A Study on Exploitable Weaknesses in QR Code Technology. Journal of Network Security. 2024; 12(2): 9–17p.

Importance of QR Code Security

While QR codes offer convenience and efficiency, their widespread use also introduces security challenges that must be addressed to protect sensitive data and prevent malicious exploitation. QR code security plays a critical role in

safeguarding financial transactions, access control systems, identity verification processes, and data exchange mechanisms. With QR codes being utilized in sensitive contexts such as mobile banking, electronic payments, and identity authentication, any vulnerabilities or weaknesses in QR code technology can have far-reaching consequences. The potential repercussions of QR code exploitation include financial losses, privacy breaches, identity theft, and reputational damage to businesses and individuals.

BACKGROUND AND RELATED WORK

History and Evolution of QR Code Technology [3–5]

Since its inception in the early 1990s by Denso Wave, a subsidiary of Toyota, QR code technology has undergone considerable advancements. Initially designed for tracking automotive parts during manufacturing, QR codes have since evolved significantly. However, their utility quickly expanded beyond industrial applications, and they gained widespread adoption in various sectors worldwide. Early iterations of QR codes were characterized by black modules arranged in a square grid against a white background. Over time, advancements in technology have led to the development of more sophisticated QR code variants, including versions capable of storing larger amounts of data and supporting additional encoding modes such as numeric, alphanumeric, byte, and kanji characters.

The standardization of QR code specifications by organizations such as the International Organization for Standardization (ISO) and the Japan Automotive Manufacturers Association (JAMA) has contributed to the interoperability and universality of QR code technology. Today, QR codes are commonly used for diverse applications, including marketing campaigns, ticketing systems, inventory management, and contactless payments.

Previous Research Efforts on QR Code Security and Vulnerabilities

Researchers and security experts have conducted extensive studies on QR code security to identify potential vulnerabilities and develop mitigation strategies. Prior studies have concentrated on different facets of QR code technology, such as:

- Analysis of QR code generation algorithms and encoding schemes to identify potential weaknesses in data representation and error correction.
- Examination of QR code parsing and decoding processes to detect vulnerabilities related to buffer overflow, format string vulnerabilities, and input validation errors.
- Investigation of potential attack vectors targeting QR code scanning applications and devices, such as malicious QR codes, URL redirection attacks, and payload injection techniques.
- Assessment of the security implications of QR code usage in critical applications, including mobile banking, electronic payments, authentication systems, and access control mechanisms.

Review of Relevant Literature and Studies Addressing QR Code Weaknesses

A comprehensive review of the existing literature on QR code security reveals a wealth of research studies, academic papers, and industry reports addressing various aspects of QR code vulnerabilities. These studies offer valuable insights into the potential risks associated with QR code usage and propose practical solutions for enhancing QR code security.

Key topics covered in the literature include:

- Analysis of specific vulnerabilities and attack scenarios affecting QR code technology, such as code injection attacks, data tampering, and social engineering exploits.
- Evaluation of existing security measures and countermeasures deployed to mitigate QR code-related threats, including QR code scanning applications, authentication mechanisms, and encryption protocols.
- Examination of emerging trends and developments in QR code security, such as the adoption of blockchain technology, biometric authentication, and machine learning techniques for QR code validation and verification.

By synthesizing and building upon the findings of previous research efforts, this study aims to contribute to the advancement of QR code security and promote the development of robust, resilient QR code systems capable of withstanding potential cyber-threats and attacks.

QR CODE FUNDAMENTALS

Explanation of QR Code Structure, Encoding Schemes, and Data Formats

QR codes are composed of black squares organized in a square grid pattern against a white backdrop. These squares encode data in two dimensions, allowing QR codes to store a wide range of information. The QR code's composition comprises three primary elements [6–8]:

- *Finder Patterns:* Square patterns positioned at three corners of the QR code assist QR code readers in accurately locating and orienting the code.
- *Alignment Patterns:* These are smaller square patterns distributed throughout the QR code, designed to assist with error correction and decoding.
- *Timing Patterns:* These consist of alternating black and white modules positioned along the edges of the QR code, serving to synchronize scanning.

QR codes employ diverse encoding methods to depict a range of data types, encompassing numeric, alphanumeric, binary, and kanji characters. Each encoding mode has specific rules for data representation and optimization. Moreover, QR codes integrate error correction features to maintain the integrity and dependability of data. Common error correction algorithms used in QR codes include Reed-Solomon codes, which can detect and correct errors caused by noise, damage, or distortion during scanning.

Overview of QR Code Generation and Decoding Processes

QR code generation involves encoding data into a QR code format using specialized software or online tools. During the encoding process, the input data is segmented and formatted according to the chosen encoding mode and error correction level. The QR code generator then adds synchronization patterns, alignment patterns, and other structural elements to create a valid QR code image.

QR code decoding, on the other hand, entails scanning and interpreting QR code images using dedicated QR code reader applications or devices. The decoding procedure consists of multiple stages:

- *Image Capture:* The QR code scanner obtains an image of the QR code through a camera or scanner.
- *Image Processing:* The captured image is processed to detect and isolate the QR code from the background and other objects.
- *Interpretation:* The QR code scanner examines the arrangement of black and white modules within the QR code image and interprets the encoded information.
- *Error Correction:* If the QR code contains errors or damage, the QR code reader utilizes error correction algorithms to recover the original data.
- *Data Extraction:* The decoded data is extracted and presented to the user or processed further, depending on the intended application.

Common Applications and Use Cases of QR Codes in Modern Society

QR codes are extensively used across diverse sectors and industries owing to their flexibility and ease of use. Some common applications and use cases of QR codes in modern society include:

- *Marketing and Advertising:* QR codes are used in advertising campaigns to provide interactive content, promotions, and product information to consumers. They enable seamless engagement between brands and customers through mobile devices.
- *Retail and E-Commerce:* QR codes facilitate mobile payments, product authentication, and inventory management in retail environments. They streamline checkout processes, enable contactless transactions, and enhance customer shopping experiences.

- In healthcare, QR codes find application in patient identification, managing medical records, labeling prescriptions, and scheduling appointments. They help healthcare providers access critical information quickly and accurately.
- *Transportation and Ticketing:* QR codes serve as electronic tickets and boarding passes for transportation services such as airlines, trains, buses, and concerts. They simplify ticket issuance, reduce paper waste, and improve ticket validation processes.
- In authentication and security, QR codes play a role in access control systems, password resets, two-factor authentication (2FA), and secure login procedures, ensuring enhanced security through user identity verification and access authorization to safeguarded assets.

Exploitable Weaknesses in QR Code Technology

Analysis of Vulnerabilities and Weaknesses in QR Code Technology

Although QR codes are extensively utilized and adaptable, they are susceptible to security vulnerabilities. In this section, we delve into some inherent weaknesses in QR code design and implementation:

- QR codes are vulnerable to data tampering, wherein malicious actors can manipulate them to either redirect users to harmful websites or modify the encoded information. For example, an attacker could overlay a legitimate QR code with a sticker containing a modified URL, leading unsuspecting users to phishing sites or malware downloads.
- *Code Injection:* Attackers can inject malicious payloads into QR codes to exploit vulnerabilities in QR code parsing and decoding mechanisms. This could include injecting JavaScript code, SQL injection payloads, or other types of malware to compromise the security of the scanning device or application.
- *Social Engineering Attacks:* QR codes can be used as a vector for social engineering attacks, where attackers trick users into scanning malicious codes. For instance, attackers may distribute QR codes via email, SMS, or physical media, enticing users with promises of discounts, prizes, or exclusive content.

Potential Attack Vectors and Security Risks

Several attack vectors and security risks are associated with QR code usage:

- *Malicious URLs:* QR codes can contain URLs that lead to phishing sites, malware downloads, or fraudulent web pages. Attackers may exploit this by distributing QR codes via email, social media, or physical media, luring users into clicking on malicious links.
- *Data Exfiltration:* Attackers can embed sensitive information, such as account credentials or personal data, into QR codes and distribute them surreptitiously. Scanning such QR codes may result in unauthorized entry to confidential data or breaches in data security.
- *Exploiting QR Code Reader Vulnerabilities:* QR code scanning applications may contain vulnerabilities that can be exploited by attackers to execute arbitrary code or compromise the security of the scanning device. For example, buffer overflow vulnerabilities or input validation errors in QR code parsing routines could allow attackers to gain control over the device.

Case Studies and Real-World Examples of QR Code Exploitation Incidents

Numerous real-world incidents demonstrate the potential risks and consequences of QR code exploitation [9–11]:

- In 2017, researchers discovered vulnerability in WhatsApp's QR code scanning feature that could be exploited to hijack user accounts. Attackers could manipulate WhatsApp's QR codes to trick users into unknowingly transferring their account to the attacker's device.
- In another incident, attackers distributed fake QR codes on public transportation systems, leading commuters to malicious websites or scam pages. These QR codes were disguised as legitimate promotions or offers, but instead, they redirected users to phishing sites or malware downloads.
- In 2020, security researchers demonstrated how attackers could use QR codes to bypass authentication mechanisms in popular mobile banking applications.

- The examples demonstrate the necessity of tackling vulnerabilities and enforcing strong security protocols to minimize the threats linked with QR code utilization. As QR codes continue to proliferate in various sectors, it is crucial for organizations and users to remain vigilant and adopt best practices for QR code security.

IMPACT AND CONSEQUENCES

Analysis of Vulnerabilities and Weaknesses in QR Code Design and Implementation [10–12]

Although QR code technology is extensively embraced, it remains susceptible to vulnerabilities and weaknesses that could be exploited by malicious actors. These vulnerabilities may arise from various factors, including design flaws, implementation errors, and shortcomings in QR code processing software. Common vulnerabilities inherent in QR code technology include:

- *Data Tampering:* QR codes can be modified or manipulated to redirect users to malicious websites, inject malicious payloads, or alter encoded data. Attackers may exploit vulnerabilities in QR code generation or decoding processes to tamper with the integrity of QR code content.
- *Code Injection:* QR codes can be used to execute arbitrary code or commands on devices scanning the code. This could lead to remote code execution, privilege escalation, or unauthorized access to sensitive information on the target device.
- QR codes might be employed in phishing schemes to deceive users into revealing sensitive information like login credentials, personal information, or financial data. Attackers can create deceptive QR codes that mimic legitimate sources, leading users to unwittingly reveal confidential information.
- *Data Leakage:* QR codes containing sensitive data, such as contact information, payment details, or personal identifiers, may be susceptible to unauthorized access or interception. Inadequate encryption or authentication mechanisms in QR code processing systems could expose confidential information to unauthorized parties.

Discussion on Potential Attack Vectors and Security Risks

The widespread use of QR codes across various sectors introduces several potential attack vectors and security risks that organizations and individuals need to be aware of:

- *Malicious QR Codes:* Attackers can distribute malicious QR codes through various channels, including printed materials, websites, emails, and social media platforms. These QR codes may contain URLs pointing to phishing sites, malware downloads, or exploit payloads, posing significant risks to unsuspecting users.
- *QR Code Spoofing:* Attackers may create counterfeit QR codes that resemble legitimate ones, leading users to scan them unknowingly. Attackers can deceive users into taking unintended actions or revealing sensitive information by manipulating QR codes, thereby jeopardizing the security of digital transactions.
- *Man-in-the-Middle Attacks:* QR codes transmitted over unsecured channels or displayed in public spaces may be intercepted by adversaries conducting man-in-the-middle attacks. Attackers can intercept QR code data, modify it in transit, or replace it with malicious content, leading to data tampering or unauthorized access.

Presentation of Case Studies and Real-World Examples

Several real-world incidents illustrate the potential consequences of QR code exploitation and the impact on individuals, businesses, and society:

- In 2019, researchers discovered a vulnerability in the Android version of WhatsApp that allowed attackers to manipulate QR codes to hijack user accounts. By taking advantage of this weakness, malicious actors could illicitly access WhatsApp accounts and intercept messages.
- In another incident, cybercriminals distributed counterfeit QR codes at a popular tourist attraction, leading visitors to malicious websites that infected their devices with malware. This attack resulted in financial losses for affected individuals and reputational damage to the tourist attraction.

- In a case of QR code phishing, attackers distributed fraudulent QR codes via email, claiming to offer discounts or promotions from reputable retailers. Unsuspecting recipients who scanned the QR codes were redirected to phishing sites designed to steal their personal information or payment details.

MITIGATION STRATEGIES AND BEST PRACTICES

Examination of Strategies for Mitigating QR Code Vulnerabilities [12–14]

To mitigate QR code vulnerabilities and enhance security, several strategies can be implemented at various stages of QR code generation, distribution, scanning, and processing:

- *QR Code Authentication:* Implement authentication mechanisms to verify the authenticity and integrity of QR codes before processing them. This may include digital signatures, cryptographic hashing, or QR code watermarking techniques to ensure that only legitimate codes are accepted.
- *Secure QR Code Generation:* Employ secure QR code generation techniques that adhere to industry standards and best practices. Use reputable QR code generation libraries or services that implement robust encryption, randomization, and error correction algorithms to generate QR codes securely.
- *Code Sanitization and Validation:* Validate QR code data input to detect and prevent malicious payloads or tampered content. Implement input validation checks, data sanitization routines, and content filtering mechanisms to sanitize QR code data before processing it.
- Promote user awareness and education regarding the potential hazards linked to QR code utilization and offer guidance on secure scanning procedures. Encourage users to verify the legitimacy of QR codes before scanning them, avoid scanning codes from untrusted sources, and exercise caution when prompted to perform sensitive actions.

Recommendations for QR Code Users, Developers, and Organizations

- User Recommendations:
  - Scan QR codes exclusively from reliable sources and ensure to authenticate the legitimacy of QR codes prior to scanning.
  - Avoid scanning QR codes that prompt for sensitive information or perform unexpected actions.
  - Keep QR code scanning applications and device firmware up to date to mitigate known vulnerabilities.
  - Report suspicious QR codes or incidents of QR code exploitation to relevant authorities or cybersecurity organizations.
- Developer Recommendations:
  - Implement secure QR code generation and parsing libraries that adhere to industry standards and security best practices.
  - Conduct thorough security assessments and code reviews of QR code processing software to identify and remediate vulnerabilities.
  - Secure sensitive data encoded within QR codes and utilize secure transmission protocols to safeguard the integrity and confidentiality of the data.
  - Deploy logging and monitoring systems to promptly identify and address security incidents related to QR codes as they occur.
- Organizational Recommendations:
  - Establish QR code security policies and guidelines to govern the usage and distribution of QR codes within the organization.
  - Conduct training and awareness initiatives for employees to educate them on QR code security risks and optimal protocols.
  - Collaborate with industry peers, standards bodies, and regulatory authorities to develop and promote QR code security standards and guidelines.
  - Comply with relevant regulations and data protection laws governing the use of QR codes, such as General Data Protection Regulation (GDPR), Peripheral Component Interconnect (PCI), Decision Support System (DSS), and Health Insurance Portability and Accountability Act (HIPAA).

Discussion on Industry Standards, Guidelines, and Regulatory Measures

Various industry standards, guidelines, and regulatory measures exist to address QR code security concerns and promote best practices:

- *ISO/IEC Standards:* The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have published standards related to QR code technology, including ISO/IEC 18004, which specifies the encoding and decoding rules for QR codes.
- *NIST Guidelines:* The National Institute of Standards and Technology (NIST) provides guidelines and recommendations for QR code security in its publications, such as NIST Special Publication 800-63, which covers authentication and identity assurance requirements for digital transactions.
- Ensure that organizations in regulated sectors, including finance, healthcare, and government, adhere to applicable rules and standards concerning QR code usage, such as PCI DSS, HIPAA, and GDPR.

FUTURE DIRECTIONS AND RESEARCH CHALLENGES

QR code technology continues to evolve, driven by emerging trends and developments aimed at enhancing functionality, usability, and security. Some notable trends and developments in QR code technology and security include [13, 14]:

- *Dynamic QR Codes:* Dynamic QR codes allow for the real-time modification of encoded data, enabling dynamic content updates and personalized experiences. This trend facilitates dynamic marketing campaigns, event management, and user engagement while also introducing new security considerations, such as data integrity and access control.
- Incorporating QR codes with blockchain technology facilitates transparent and secure data transactions, improving traceability, authenticity, and auditability. Blockchain-enabled QR codes find application in supply chain management, product authentication, and digital asset management, providing immutable records and decentralized verification methods.
- Combining QR codes with biometric authentication techniques like fingerprint or facial recognition strengthens security by introducing an extra layer of identity verification. Biometric-enabled QR codes find utility in secure access control systems, identity verification procedures, and mobile banking apps, providing heightened security and user convenience.
- Incorporating QR codes with augmented reality (AR) technologies allows for interactive and immersive experiences, connecting the physical and digital realms. AR-enabled QR codes are used in marketing campaigns, educational materials, and gaming applications, offering engaging and interactive content experiences while introducing new security challenges related to data privacy and content integrity.

Research Gaps and Challenges in Addressing QR Code Weaknesses

Despite advancements in QR code technology and security, several research gaps and challenges persist, including:

- *Usability versus Security Trade-offs:* Balancing usability with security remains a challenge in QR code design and implementation. Simplifying QR code scanning processes to enhance user experience may inadvertently introduce security vulnerabilities, requiring careful consideration of trade-offs between usability and security.
- *Standardization and Interoperability:* Lack of standardized protocols and interoperability standards hinders seamless integration and adoption of QR code technology across different platforms and systems. Addressing interoperability challenges requires collaboration among stakeholders to develop common standards and guidelines for QR code usage.
- *Privacy Concerns:* QR codes often contain sensitive information, raising privacy concerns related to data collection, tracking, and unauthorized access. Protecting user privacy while enabling efficient QR code usage requires robust privacy-enhancing technologies, such as data anonymization, encryption, and consent management mechanisms.

Future Research Directions and Innovation in QR Code Security

To address the aforementioned research gaps and challenges, future research in QR code security could focus on the following areas:

- Creating improved authentication mechanisms like multi-factor authentication and biometric verification to bolster QR code security and thwart unauthorized access.
- *Secure QR Code Processing Algorithms:* Designing secure QR code processing algorithms that prioritize data integrity, error detection, and resistance to tampering or manipulation.
- *Privacy-Preserving QR Code Solutions:* Investigating privacy-preserving QR code solutions that protect user privacy while enabling secure data transactions and interactions.
- *Blockchain-Based QR Code Security:* Exploring the integration of blockchain technology with QR codes to provide decentralized verification, traceability, and transparency for secure data transactions.
- *Machine Learning for QR Code Security:* Leveraging machine learning techniques for anomaly detection, threat analysis, and predictive security analytics to detect and mitigate QR code-related security threats proactively.

CONCLUSION

Throughout this study, we have delved into the realm of QR code technology, examining its structure, applications, vulnerabilities, and security considerations. Important discoveries from our investigation reveal that QR codes have permeated modern culture, fulfilling diverse roles in sectors such as marketing, retail, healthcare, transportation, and authentication. While QR codes have been widely adopted, they are still susceptible to vulnerabilities and weaknesses that malicious actors could exploit. These vulnerabilities include data tampering, code injection, phishing attacks, and data leakage. The exploitation of QR code vulnerabilities can have significant consequences for individuals, businesses, and society, including financial losses, data breaches, privacy violations, and reputational damage. Mitigating QR code vulnerabilities requires a multifaceted approach, including the implementation of authentication mechanisms, secure QR code generation practices, code sanitization and validation, user awareness programs, and compliance with industry standards and regulations. In recapitulation, addressing exploitable weaknesses in QR code technology is of paramount importance for maintaining trust and security in digital transactions. As QR codes continue to play an integral role in our daily lives, safeguarding against potential threats and vulnerabilities is essential to protect sensitive data, preserve privacy, and mitigate financial and reputational risks. The importance of QR code security cannot be overstated, and the need for continuous vigilance and improvement is evident. By staying abreast of emerging threats, adopting best practices, and fostering collaboration among stakeholders, we can bolster QR code security and ensure the integrity, authenticity, and trustworthiness of QR code-based interactions. Let us remain vigilant, proactive, and committed to enhancing QR code security to safeguard against evolving cyber threats and preserve the integrity of digital transactions in an increasingly interconnected world.

REFERENCES

1. Dabrowski A, Krombholz K, Ullrich J, Weippl ER. QR inception: barcode-in-barcode attacks. In: Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices, Scottsdale, AZ, USA, November 7, 2014. pp. 3–10.
2. Han X, Zhang Y, Zhang X, Chen Z, Wang M, Zhang Y, Ma S, Yu Y, Bertino E, Li J. Medusa attack: exploring security hazards of in-app QR code scanning. In: 32nd USENIX Security Symposium (USENIX Security 23), Anaheim, CA, USA, August 9–11, 2023. pp. 4607–4624.
3. Tribak H, Gaou M, Gaou S, Zaz Y. QR code recognition based on HOG and multiclass SVM classifier. Multimedia Tools Appl. 2023; 83 (17): 1–30.
4. Lin D, Stamp M. Hunting for undetectable metamorphic viruses. J Computer Virol. 2011; 7: 201–214.

5. Mannan M, Barrera D, Brown CD, Lie D, Van Oorschot PC. Mercury: recovering forgotten passwords using personal devices. In: Financial Cryptography and Data Security: 15th International Conference, FC 2011, Gros Islet, St. Lucia, February 28–March 4, 2011. Revised Selected Papers 15 Berlin, Germany: Springer; 2012. pp. 315–330.
6. Kals S, Kirda E, Kruegel C, Jovanovic N. SecuBat: a web vulnerability scanner. In: Proceedings of the 15th International Conference on World Wide Web, Edinburgh, Scotland, May 23–26, 2006. pp. 247–256.
7. Ali H, Kharade KG, Kamat RK. An analysis and evaluation of vulnerability assessment tools. Cyberpsychol Behav Soc Netw. 2022; 25 (4): 448–456.
8. Vuagnoux M, Pasini S. An improved technique to discover compromising electromagnetic emanations. In: 2010 IEEE International Symposium on Electromagnetic Compatibility, Fort Lauderdale, FL, USA< July 25–30, 2010. pp. 121–126.
9. Elbaz L, Bar-El H. Strength Assessment of Encryption Algorithms. White Paper. Kefar Netter, HaMerkaz, Israel: Discretix Technologies Limited; 2000.
10. Viega J, Bloch JT, Kohno T, McGraw G. Token-based scanning of source code for security problems. ACM Trans Inform Syst Security. 2002; 5 (3): 238–261.
11. Phillips SK. Creating Feedback Channels with Optical Communications for Information Operations (IO). Doctoral Dissertation. Monterey, CA, USA: Naval Postgraduate School; 2016. Available at https://core.ac.uk/download/pdf/45464713.pdf
12. Blaze M. Election integrity and technology: vulnerabilities and solutions. Georgetown Law Technol Rev. 2019; 4: 505–522.
13. Black PE, Kass M, Koo M, Fong E. Source code security analysis tool functional specification version 1.0. Washington, DC, USA: US Department of Commerce, National Institute of Standards and Technology; 2007.
14. Bletsch T, Jiang X, Freeh V. Mitigating code-reuse attacks with control-flow locking. In: Proceedings of the 27th Annual Computer Security Applications Conference, Orlando, FL, USA, December 5–9, 2011. pp. 353–362.

