QR Code Security Analysis
Review of Current Solutions

Abbie Barbir

See Reference 7.

QR Codes as Attack Vectors

Basically Static offline or online attacks

1. The attacker replaces the entire QR code. An attacker creates a new QR code with a malicious link encoded and pastes it over an already existing one on e.g. a billboard advertisement.

2. Attacker modifies individual modules of a QR code. Encoded content is modified solely by changing the color of specific modules of the QR Code to which the user will be directed after scanning the code.

QR Code Requirements Security Requirements

1. Visual QR Codes (help user identify fraud in QR)
2. Digital Signatures as means to secure QR code content (no specific method proposed)
3. Secure Code Reader application (days when application needed to be downloaded from app store)
4. Browser support of Malicious URL detection
5. Content display on QR code (tell user what the code is doing)
6. Support of anti-phishing (No specific)
SECURITY ANALYSIS OF MOBILE AUTHENTICATION USING QR-CODES

See Reference 2.

QR-TANs is a transaction authentication technique based on QR-Code, allow the user to directly validate the content of a transaction within a trusted device.

Figure 1. Basic procedure of Authentication Center based Architecture
SECURITY ANALYSIS OF MOBILE AUTHENTICATION USING QR-CODES

See Reference 2.

Figure 2. Basic procedure of Mobile Application based Architecture
SECURITY ANALYSIS OF MOBILE AUTHENTICATION USING QR-CODES

Attack Models
• Internal and external attacks
  1. QR-Code Cloning
  2. Authentication Hijacking
  3. Stored Data Exfiltration
  4. Internal Algorithm Disclosure
  5. Network Message Eavesdropping
  6. Communication Protocol Vulnerabilities

• RECOMMENDATIONS FOR SECURE IMPLEMENTATION
  1. Expiring QR-Code Available Period
  2. Maintain Local Storage Cleanliness (limit sensitive data in QR code)
  3. Deliberate Data Storing (encrypt data storage)
  4. Obfuscation
  5. Rogue Access point detection, Malware detection / device security (Finger printing)

Does NOT solve Real MITM Attacks

See Reference 2.
QR-Tan: Secure mobile transaction authentication

See Reference 4

- Starnberger et al.
- QR-TAN, a transaction authentication method based on QR codes and a trusted mobile device.
  - A shared secret key installed in user mobile device and the server.
    - private key is stored in the mobile device and the untrusted computer has access to the public key
- To perform a transaction,
  - a nonce is requested from the server.
  - The untrusted computer then encrypts transaction information and the nonce using the mobile device's public key and displayed the result as a QR code.
  - The mobile device scans the QR code to obtain the encrypted information, which it is required to decrypt using its private key.
  - It then computes a hash based on the transaction information, the nonce, and whether the user approves or rejects the transaction. Part of this hash is sent as a TAN to the server, which computes its own approve and reject hash values, and tries to match these with the value computed on the mobile device.

Basically, Private key in Mobile device encrypt the transaction, so MITM cannot see the details
See Reference 1.

"A MOBILE BASED ANTI-PHISHING AUTHENTICATION SCHEME USING CHALLENGE-RESPONSE AND QUICK RESPONSE CODE"

- Does NOT solve Real MITM Attacks
- None Functional
Authentication and Transaction Verification using QR Codes with a Mobile Device

See Reference 4

- Mobile phone hold private key
- Server send OTP secured to client
- Client decode via private key on smart phone
- Assume: Mobile device offline
- Client connect with a session key to server see Figure 2

Fig. 1. Overview of the user authentication phase.
See Reference 4

- Client connect with a session key to server, see Figure 2
- Session data encrypted by private key

**Fig. 2.** Overview of the transaction verification steps.
QRLJacking

- **QRLJacking** or Quick Response Code Login Jacking is a simple social engineering attack vector capable of session hijacking affecting all applications that rely on “Login with QR code” feature as a secure way to login into accounts. In a simple way, In a nutshell victim scans the attacker’s QR code results of session hijacking.

- Go to [https://owasp.org/www-community/attacks/Qrljacking](https://owasp.org/www-community/attacks/Qrljacking) during presentation

- SQRL Project
- What is QRLJacking Attack?
- QRLJacking or Quick Response code Login Jacking is a simple-but-nasty attack vector affecting all the applications that relays on “Login with QR code” feature as a secure way to login into accounts, In a simple way, It’s all about convincing the victim to scan the attacker’s QR code.
References


2. Siwon Sung, Joonghwan Lee1, Jinmok Kim, Jongho Mun2 and Dongho Won, “SECURITY ANALYSIS OF MOBILE AUTHENTICATION USING QR-CODES”, Samsung Electronics and Sungkyunkwan University. DOI : 10.5121/csit.2015.51612

3. Authentication and Transaction Verification using QR Codes with a Mobile Device

Yang-Wai Chow1, Willy Susilo1, Guomin Yang1, Man Ho Au2 and Cong Wang3

1 Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, Wollongong, Australia {caseyc, wsusilo, gyang}@uow.edu.au
2 Department of Computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong csallen@comp.polyu.edu.hk
3 Department of Computer Science, City University Hong Kong, Kowloon Tong, Hong Kong congwang@cityu.edu.hk
References


6. Secure Authentication for Online Banking Using QR Code

Sonawane Shamal1, Khandave Monika2, Nemade Neha3

B.E computer engineering, Institute of Knowledge College of engineering, pune
References


Katharina Krombholz, Peter Frühwirt, Peter Kieseberg, Ioannis Kapsalis, Markus Huber, Edgar Weippl
[1stletterfirstname]@sba-research.org

SBA Research, Vienna

8.