Life of a QR code. To scan or not to scan, that is the question?

Warren Finch
How to use QR code
QR Code is an abbreviation for Quick Response code; it is a type of 2D barcode; invented in 1994 by a Japanese automotive company named Denso Wave; consists of a set of square dots arranged in a square grid pattern with white background.
<table>
<thead>
<tr>
<th>Developer (Country)</th>
<th>QR Code</th>
<th>PDF417</th>
<th>DataMatrix</th>
<th>Maxi Code</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DENSO (Japan)</td>
<td>Symbol Technology (USA)</td>
<td>RVSI Acuity CiMatrix (USA)</td>
<td>UPS (USA)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th><img src="image" alt="QR Code Example" /></th>
<th><img src="image" alt="PDF417 Example" /></th>
<th><img src="image" alt="DataMatrix Example" /></th>
<th><img src="image" alt="Maxi Code Example" /></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Matrix</th>
<th>Stacked Bar Code</th>
<th>Matrix</th>
<th>Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Numeric</td>
<td>7,089</td>
<td>2,710</td>
<td>3,116</td>
<td>138</td>
</tr>
<tr>
<td>Alphanumeric</td>
<td>4,296</td>
<td>1,850</td>
<td>2,355</td>
<td>93</td>
</tr>
<tr>
<td>Binary</td>
<td>2,953</td>
<td>1,018</td>
<td>1,556</td>
<td>-</td>
</tr>
<tr>
<td>Kanji</td>
<td>1,817</td>
<td>554</td>
<td>778</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Capacity</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Numeric</td>
<td>- Large Capacity</td>
<td>- Large Capacity</td>
<td>- Small Size</td>
<td>- High Speed Scan</td>
</tr>
<tr>
<td>Alphanumeric</td>
<td>- Small Size</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Binary</td>
<td>- High Speed Scan</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kanji</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Main Features</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Numeric</td>
<td>- AIM International</td>
<td>- AIM International</td>
<td>- AIM International</td>
<td>- AIM International</td>
</tr>
<tr>
<td>Alphanumeric</td>
<td>- JIS</td>
<td>- ISO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Binary</td>
<td>- ISO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kanji</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standardization</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Numeric</td>
<td>- AIM International</td>
<td>- AIM International</td>
<td>- AIM International</td>
<td>- AIM International</td>
</tr>
<tr>
<td>Alphanumeric</td>
<td>- JIS</td>
<td>- ISO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Binary</td>
<td>- ISO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kanji</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Rise of the QR code

• 2011 - 6.2% of people used a QR code in the USA
• 2016 - $5.5 trillion paid with smartphones in China, compared to $112 billion in USA. **WeChat Wallet** was only released in China in 2015
• 2017 - Visa, Mastercard and Amex combined to launch the world’s first interoperable QR code acceptance system. That was in India.
• 2017 - EMV card payment specs, unveiled two QR code payment specifications – one for merchant-presented codes, one for and consumer-presented.
• Any camera phone can scan them, and the cost of displaying them for a merchant is virtually zero

A QR 2D bar code as specified by [ISO/IEC 18004:2015]
QR code usage

- Autonomous vehicles / systems
- Payment systems
- Sharing information
- Ticketing systems
Lost in Translation

https://myFakeWhatsApp.site
Attack vectors / infection points

- Phishing attacks
- Malicious software distribution
- Redirect to malicious site
- **Physical Tampering**
- Replacing the QR code
- Impersonation
Attack vectors / infection points

MalQR is a collection of malicious QR Codes & Barcodes that can be used to test the security of scanners and applications

• SQLi
• XSS
• Command injection
• Fuzzing

https://malqr.shielder.it
Attack vectors / infection points

• QRLJacking

https://www.owasp.org/index.php/Qrljacking
Attack vectors / infection points

- QRLJacking

https://www.youtube.com/watch?time_continue=349&v=4QwyBXiZhG0

https://github.com/OWASP/QRLJacking
iOS camera QR code URL parser bug

I've learned recently that the iOS 11 camera app will now automatically scan QR codes and interpret them. This is pretty cool, until now you needed special apps to do that for you on iOS. When scanning a QR code which contains a URL – in this case https://infosec.rm-it.de/ – iOS will show a notification like this:

![Notification showing a QR code](image)

Naturally the first thing I want to try is to construct a QR code which will show an unsuspicious hostname in the notification but then open another URL in Safari.

And this is exactly what I found after a few minutes. Here it is in action:

![QR Code with modified URL](image)

https://xxx\@facebook.com:443\@infosec.rm-it.de/
Creating QR codes

- Determine which encoding mode to use
- Encode the data
- Generate error correction codewords
- Interleave blocks if necessary
- Place the data and error correction bits in the matrix
- Apply the mask patterns and determine which one results in the lowest penalty
- Add format and version information

https://developers.google.com/chart/infographics/docs/qr_codes
What makes a QR code

Rebuild a QR code

https://medium.freecodecamp.org/lets-enhance-how-we-found-rogerkver-s-1000-wallet-obfuscated-private-key-8514e74a5433
Protect Against Malicious QR Codes

• Observe before use
• Look at URL before proceeding
• Be suspicious
• Never give personal or login information
• Use a QR code scanner that has security features
Disable QR code scanning
Security features for QR Codes

- Q Platform
- SQRC
- FrameQR
- Q-revo trace
- Q-revo protection
Q Platform

- A cloud server that generates, reads, and logs QR Code
SQRC


• A single QR Code can carry public data and private data.
Cloud integration

- Q-revo protection
- Checking authenticity
- Q-revo trace
- Traceability service
FrameQR

- Released in Oct 2014
- A combination of a hologram and QR Code which can be used for anti-forgery measures and traceability.
- Is not compatible with normal QR Codes and requires different software to generate and read the codes
QR Code Reader “Q”

- To read the newer features, get the latest QR code reading software
  - https://itunes.apple.com/jp/app/%E5%85%AC%E5%BC%8Fqr%E3%82%B3%E3%83%BC%E3%83%89%E3%83%AA%E3%83%BC%E3%83%80%E3%83%BC-\ q/id911719423?mt=8

<table>
<thead>
<tr>
<th>Supported Smartphones</th>
<th>Android / iPhone (iOS 7 or later)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Price</td>
<td>Free</td>
</tr>
<tr>
<td>Supported Codes</td>
<td>2D codes QR Code models 1 and 2 (GS1 format), Micro QR Code, SQRC, FrameQR, and MapQR</td>
</tr>
<tr>
<td></td>
<td>Bar codes AN-13, EAN-8 (JAN-13 and JAN-8), UPC-A, UPC-E, and UPC/EAN with add-ons</td>
</tr>
</tbody>
</table>