Malware and QR Codes

Mauro A. de los Santos Nodar
Adrián Martínez Bemposta

Mentored Work - Malware Analysis

April 26th, 2022

Content

1 Introduction
- Purpose and Aims
- Technology

2 Incidents
- Examples of attacks

3 Vulnerabilities and Exploits
- Common vulnerabilities

4 Lab part
- Cases of use
- Real Time/Video Demo

5 Mitigation and Contermeasures

6 Conclusions

Introduction

Purpose and Aims

Purpose

- Demonstrate the importance of security in QR Codes
- Study a current malware entry vector and cibersecurity topic

Purpose and Aims

Purpose

- Demonstrate the importance of security in QR Codes
- Study a current malware entry vector and cibersecurity topic

Aims

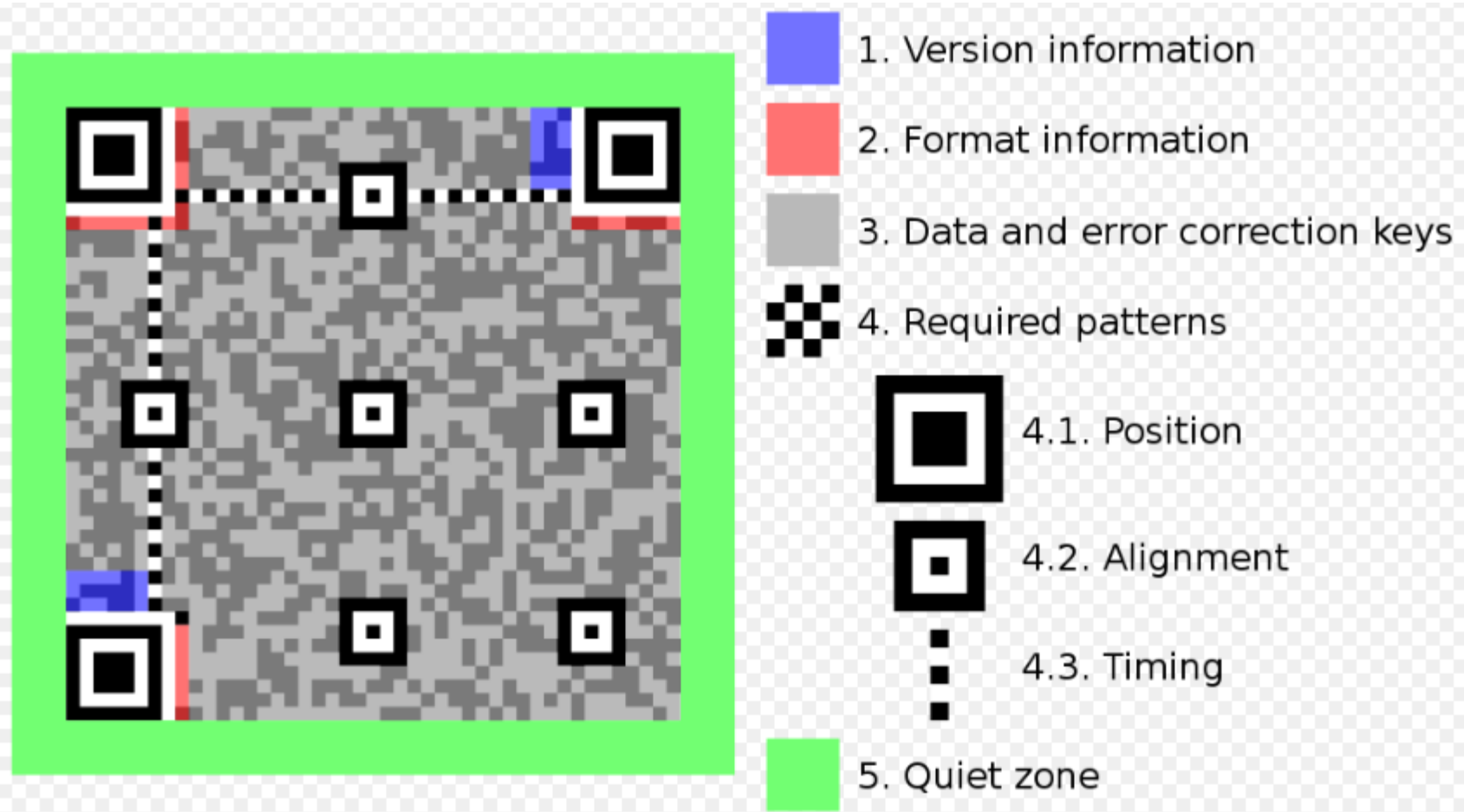
- Deeper knowledge in QR Codes
- Understand the vulnerabilities
- Exploit those vulnerabilities
  - Showing recent past attacks
  - Attacking ourselves using QR Codes
- Learn how to secure QR Codes

Technology

QR Codes: What are they?

- *Quick Response Code*
- Invented in 1994 by a Japanese automotive company (D. Wave)
- 2D Coded information
- Up to 3Kb of data (177 x 177 is the maximum)
- 40 versions. 21 x 21 the 1st one. 4 x 4 jumps
- Error-correcting algorithm

Technology


1. Version information
2. Format information
3. Data and error correction keys
4. Required patterns
4.1. Position
4.2. Alignment
4.3. Timing
5. Quiet zone

Technology

Version 1 (21×21). Content: "Ver1"

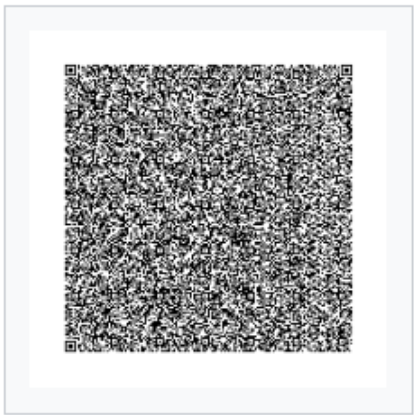
Version 2 (25×25). Content: "Version 2"

Version 3 (29×29). Content: "Version 3 QR Code"

Version 4 (33×33). Content: "Version 4 QR Code, up to 50 char"

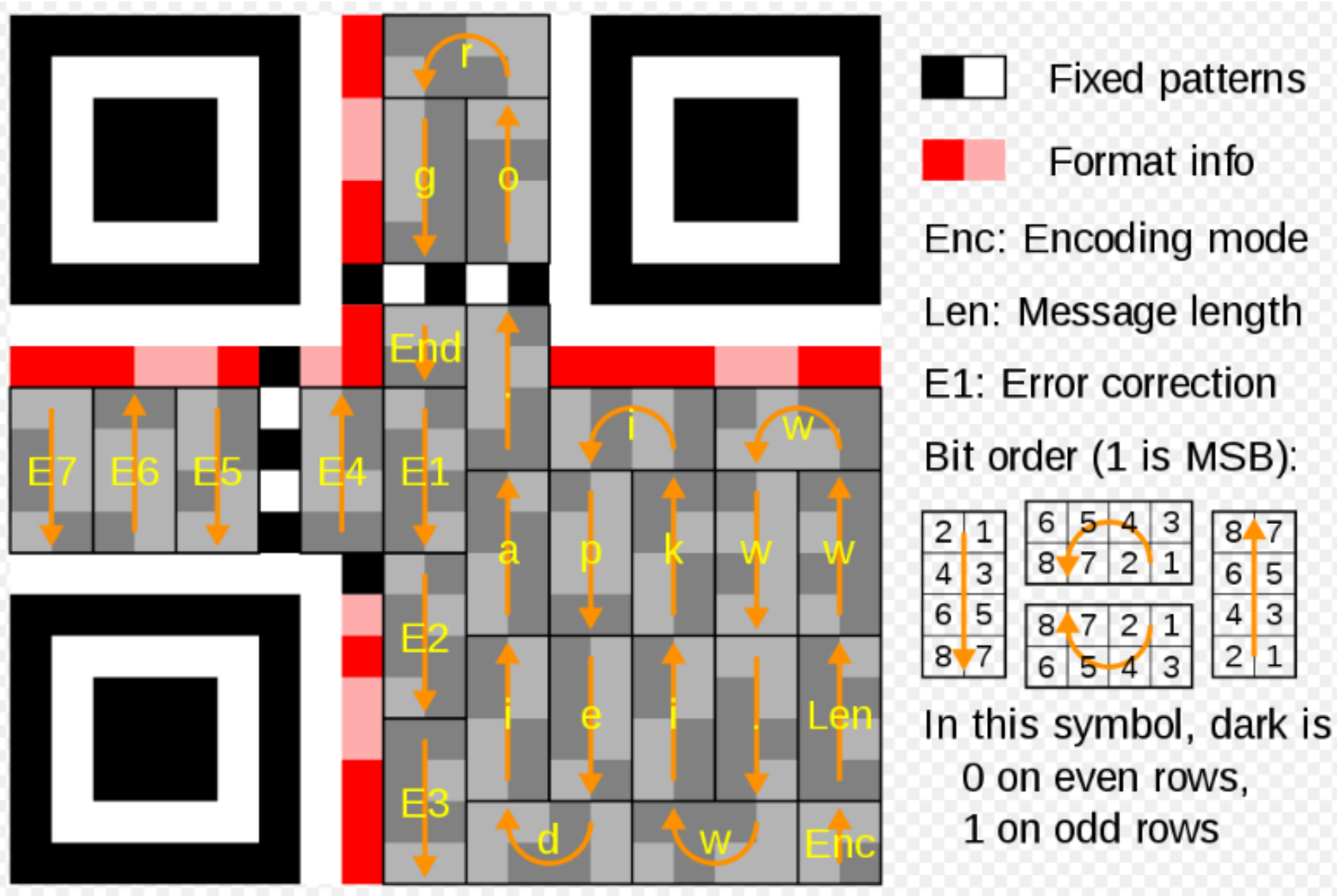
Version 10 (57×57). Content: "VERSION

Version 25 (117×117) Content: 1,269



Version 40 (177×177)

Technology


r
g
o
End
E7
E6
E5
E4
E1
i
w
a
p
k
w
w
E2
i
e
i
Len
E3
d
w
Enc
Fixed patterns
Format info
Enc: Encoding mode
Len: Message length
E1: Error correction
Bit order (1 is MSB):
In this symbol, dark is
0 on even rows,
1 on odd rows

Incidents

Examples of attacks

Recent incidents

- Massive growth of QRs due to COVID-19
- More and more usual in ciberattacks
- *Quishing* and Social Engineering
  - Fake legit and secure image
  - The victim is who does the action
  - Curiosity
  - Everyone has a QR scanner in their hands

News and attacks

Home › News › Security

FBI: Hackers Are Compromising Legit QR Codes to Send You to Phishing Sites

The scheme exploits how QR codes have grown in popularity during the pandemic.

By Michael Kan January 19, 2022

Quebec Says The QR Codes Are Still Secure After Politicians' Codes Were Reportedly Hacked

The Ministry of Health said the police have been contacted.

Thomas MacDonald
Senior Editor

August 27, 2021, 10:19 AM

News and attacks

Vulnerabilities and Exploits

Common vulnerabilities and exploits

Common vulnerabilities

- Can carry URL data type
- Automatic URL open when they are read
- Permissive readers
- They are easy to create
- They could be anywhere
- They do not have own security measures (integrity or authenticity)

Common vulnerabilities and exploits

Common vulnerabilities

- Can carry URL data type
- Automatic URL open when they are read
- Permissive readers
- They are easy to create
- They could be anywhere
- They do not have own security measures (integrity or authenticity)

Common exploits

- *Quishing* and *QRLjacking*
- Malware download
- Command execution
- Change color of concrete squares

Lab part

Cases of use

1. Hacking with QRgen

- Python based tool
- Autogenerated QR payloads
- Multiple types: SQLi, XSS, LFI...
- Customized exploits

Cases of use

1. Hacking with QRgen

- Python based tool
- Autogenerated QR payloads
- Multiple types: SQLi, XSS, LFI...
- Customized exploits

2. More elaborated attacks

- Customized attacks
- WiFi connection
- Malicious website tailor-made
- Using Setoolkit and Metasploit [Practice 4]

Video Demo

Mitigation and Contermeasures

Mitigation and Contermeasures

Avoiding the attacks

- Secure backend against command injection
- Check insecure sources: WiFis, websites, APKs...
- Legit QR Scanners and secured QR-based login systems

Mitigation and Contermeasures

Avoiding the attacks

- Secure backend against command injection
- Check insecure sources: WiFis, websites, APKs...
- Legit QR Scanners and secured QR-based login systems

Securing QR Codes

- SQR Codes
- CIA plugins
- Victim-side measures

Conclusions

Conclusions

Main aspects

- Massive growth of every aspect related to QRs
- Technology with great potential
- Important security component
- Risky, vulnerable and not easy to secure
- The human side is the most important

Credits

Mauro

- Presentation organization and format
- Technology study and incident research
- Vulnerabilities and exploits research
- QRGen
- General countermerasures
- Conclusions

Adrián

- Cases of use choosing
- Implementation of lab part
- Video production
- Video editing
- Avoiding the attacks
- Conclusions

References

Theory

1. https://en.wikipedia.org/wiki/QR_code
2. http://qrcode.meetheed.com/question14.php?s=s
3. https://cisomag.eccouncil.org/how-cybercriminals-exploit-qr-codes-to-their-advantage/
4. https://www.researchgate.net/publication/221593120_QR_code_security
5. https://courses.csail.mit.edu/6.857/2014/files/12-peng-sanabria-wu-zhu-qr-codes.pdf
6. https://publications.sba-research.org/publications/llncs.pdf
7. https://www.csa.gov.sg/singcert/publications/quick-response-code-related-cyber-threats
8. https://simple.wikipedia.org/wiki/SQR_codes

References

Practice

1. https://null-byte.wonderhowto.com/how-to/create-malicious-qr-codes-hack-phones-other-scanners-0197416
2. https://www.youtube.com/watch?v=Tjc-Xs-1fq8
3. https://www.hackeracademy.org/how-to-hack-using-qr-codes/
4. https://medium.com/@andrearebora/how-to-hack-an-android-phone-using-qr-codes-fc71428630e
5. https://thehackernews.com/2016/07/qrljacking-hacking-qr-code.html
6. https://www.elespanol.com/omicrono/tecnologia/20211008/codigos-qr-nuevo-grial-hackers-roban-dinero/615189363_0.html
7. https://resources.infosecinstitute.com/topic/security-attacks-via-malicious-qr-codes/
8. https://www.esecurityplanet.com/threats/qr-code-security-problem/

Malware and QR Codes

Mauro A. de los Santos Nodar
Adrián Martínez Bemposta

Mentored Work - Malware Analysis

April 26th, 2022