qrypt0 - encrypted short messages exchanged between offline computers

Andreas O. Bender
www.andreasobender.org
andreasobender@mac.com

December 4, 2017

Abstract

A system is described for exchanging encrypted short messages between computers which remain permanently isolated from any network accessible to the attacker. The main advantage is effective protection of these computers from malware which could circumvent the encryption. For transmission, the ciphertext is passed between isolated and connected computers in the form of a QR code[1], which is displayed on and scanned from a screen. The security of qrypt0 therefore rests on the cryptography and the computer's physical isolation rather than on the computer security of the encrypting device.

1 crypto on networked devices

Message encryption is usually carried out on networked computers. This is hardly every questioned as a means to transmit the ciphertext from Alice to Bob, even though it allows an attack which is not directed at the cryptography: It is directed at the endpoints which carry out the encryption.

This is highly relevant in view of the fact that rather than attacking the encryption, circumventing it is often much easier. Six possibilities for doing so are listed in [1]. Four of them consist of guessing, finding or compelling the key and locating the plaintext. Defending against these circumventions is possible by the corresponding measures of choosing a key of sufficient entropy, protecting the key and keeping track of all copies of the plaintext.

[1] "QR Code" is a registered trademark of DENSO WAVE INCORPORATED.

The plaintext must of course be stored on the encrypting device for at least some time. Therefore the other two possibilities of circumventing encryption are hard to defend against: exploiting a flaw in the encrypting device and accessing the plaintext when in use. In practice attackers use vulnerabilities of the operating system for things like the installation of keyloggers which record the plaintext as it is typed in.

Some known examples of such attacks are recently disclosed activities in the program Vault 7 by the United States' Central Intelligence Agency [2]. The German Federal Intelligence Service BND has started a program to circumvent encryption in various popular messengers [3].

Vulnerabilities which are not publicly known, so-called Zero-Days, are traded continuously by companies like Zerodium [4]. Security patches are released for the gaps which do become public knowledge. However, the author is not aware of any producers of system software who are even prepared to suggest, let alone give an assurance that there are no more such vulnerabilities hidden in their software.

Operating systems impervious to infection by malware appear to be a long way off [5, chpt. 8] [6, 20.6].

We need a system with the following properties:

- The exchange of encrypted messages can be protected effectively against circumvention of the encryption. In particular, security vulnerabilities in the operating system of the encrypting computer do not compromise the system's security.

- The attacker sees only the number of messages, their timing and the ciphertext.

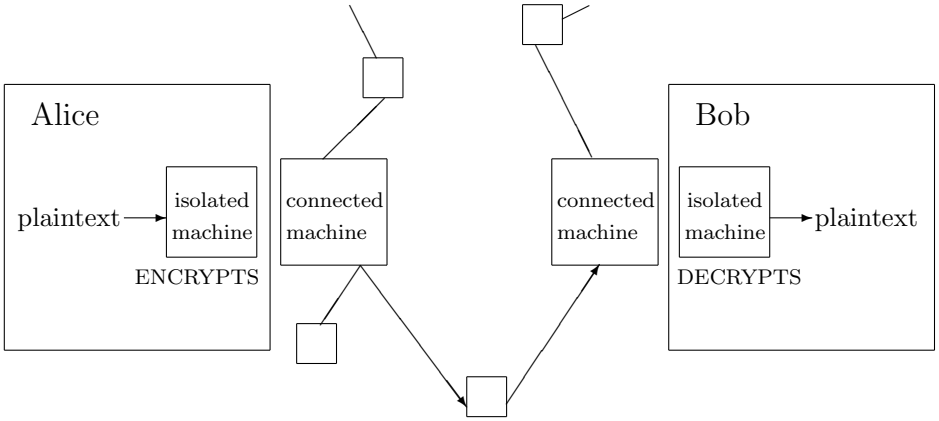
Relying only on currently available technology, compromises regarding convenience are to be expected. Even so, for high-value data a system offering this level of security with some inconvenience is still much better than what has been available up to now.

2 qrypt0 on isolated devices

The distinguishing feature of qrypt0 is the isolation of the encrypting computer from any open network and the transmission of the ciphertext encoded in a QR code. This barcode is displayed on Alice's screen and scanned into a connected computer which sends it on to Bob.

This isolation from the network provides effective protection against remote infection with malware. Keeping the isolated computer physically secure is necessary to protect it from local infection with malware.

The website [7] links to a freely available prototype, which includes a discussion of implementation issues.



2.1 Functionality

Message encryption. The message is entered into the isolated computer by Alice. The system adds a message number and a timestamp. The message is authenticated, padded up to the maximum length for one barcode and encrypted. The resulting ciphertext is encoded in a QR code.

Message transmission. An online device under Alice's control scans in the QR code from the screen of the isolated computer and transmits the barcode itself or the ciphertext to the recipient by any means available.

Message decryption. An online device under Bob's control receives the message containing the ciphertext. If necessary, this device encodes the ciphertext into a QR code and displays it on screen. Bob's isolated computer scans in the QR code, decodes and decrypts the message, removes the pad and checks the authentication.

2.2 Design choices

The main cost of the system consists of one additional computer per user and a limit on the length of the message which one QR code can contain. The QR code has the largest capacity of 2953 bytes among common 2-dimensional barcodes. Note that this includes the characters needed for formatting purposes, for authentication, the message number and a timestamp.

Installation. In order to avoid infection with malware, the necessary software should be installed by burning it onto an optical disk, transferring it to the isolated machine from that medium and then checking its authentication.

Cryptography. The system can be used with both asymmetric and symmetric cryptography. Using only symmetric cryptography requires a preshared key, but has the advantage of simplicity. No understanding of handling public and private keys is required.

If asymmetric cryptography is used, key material can be entered by scanning QR codes, where more than one may be required.

Formatting. In order to be sure no messages got lost, a message number should be added. Management of messages is easier to organize if also a timestamp is included.

Authentication. This can be done using a symmetric key for a hash-based message authentication code. The choice of whether encryption or authentication is done first has to be made.

Message length. We recommend padding the message up to its maximal length, since information about the message length may be valuable to an attacker.

Note that no information on the message is transmitted by the system except the ciphertext itself. In particular, the file name has to be chosen anew after passing the ciphertext between two computers by scanning in a QR code.

System use information. Either the QR code itself or the ciphertext it contains can be transmitted. Transmitting the QR code itself passes information on system use to an attacker.

Plaintext storage. As mentioned above, one way of circumventing encryption consists of locating copies of the plaintext. As protection against this, we recommend to do a secure erase of the plaintext messages after display and to retain only the ciphertext on secondary storage.

System advantages:

- The only way the system can be compromised by malware after installation is by gaining physical access to the isolated computer.
- Sidechannel attacks using timing information or measurement of power consumption are only possible with physical access to the isolated computer while the system is running.
- In case only symmetric cryptography is used, the system is easy to handle. The key consists of a sufficiently long passphrase. Neither management of keys on secondary storage nor an understanding of asymmetric cryptography is necessary.

System limitations:

- One QR code can contain at most 2953 bytes, including some bytes used for formatting. Depending on the scanning device used, the limit can be about half that number.
- Every user needs an isolated computer.
- The isolated computer needs to be kept physically secure.

Attacks:

- Evil maid attack. Anyone who has physical access to the isolated computer can install malware. Such a program can establish and use a hidden channel in the QR code or other sidechannels like the loudspeaker or flashing lights.
- RF emissions of the isolated machine as side channel.
- Traffic analysis. The attacker can see the number and timing of transmitted messages.
- Ciphertext-only attack on the cipher itself.

References

[1] Orin S. Kerr, Bruce Schneier. Encryption workarounds. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033

[2] https://wikileaks.org/ciav7p1/ Released March 7, 2017.

[3] https://netzpolitik.org/2016/projekt-aniski-wie-der-bnd-mit-150-millionen-euro-messenger-wie-whatsapp-entschluesseln-will/

[4] http://www.zerodium.com

[5] Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. Cryptography engineering. *Wiley Publishing 2010.*

[6] Matt Bishop. Computer security: art and science. *Addison-Wesley 2002.*

[7] www.andreasobender.org