

Encrypted QR Code

Summary of Research Papers

Course Title:

- Information System Security - CS 446

Course Instructor:

- Dr. Sufian Hameed

Group Members:

- Mehdi Raza Rajani k163904 (Group Leader)
- Junaid Mazhar Muhammad k163878
- Tahir Raza Hemani k163905

Purpose of Document:

- The first deliverable of the Semester Project.

Date of Submission:

Saturday, November 23rd, 2019

Summary of Research Papers:

Research Paper 1:

Title:

QR Code Security: A Survey of Attacks and Challenges for Usable Security

Reference:

Krombholz, Katharina, et al. "QR code security: A survey of attacks and challenges for usable security." International Conference on Human Aspects of Information Security, Privacy, and Trust. Springer, Cham, 2014.

Summary:

QR Codes are two-dimensional barcodes that are used to transmit information across all over the world. QR Code is used in daily life for the purpose of advertising, mobile payments, access control, and navigation. A person can easily encode the information in a QR Code and the recipient can decode it from a simple QR Code Scanner by scanning the QR Code. QR Code has made the transmission of information to easy. On the contrary, the security risks are also increasing which should be tackle at earliest.

In the past few years, the number of incidents was witnessed in which the QR Code was falsely modified for the purpose of phishing and stealing sensitive personal information. Sometimes the QR Code is fully changed and sometimes some masking is changed so that the recipients reach to false URL.

The research paper discusses a number of solutions for protecting the user from getting affected. Firstly, the use of the Visual QR Code and digital signature can protect the user to get affected. Secondly, the Service Layer can be improved by masking the QR Code and detecting malicious URL. Lastly, by taking care of Usability Requirements user can be prevented through Content Preprocessing, Antiphishing tools, and Content Verification that the content is good enough to be displayed or not.

Through these measures, the major chunk of the affected user can be saved but still there need to be done something else to increase the security of the QR Code may be encrypting them, this is the Open Research Challenge by the author.

Research Paper 2:

Title:

Encrypted QR Code

Reference:

https://www.ieee-security.org/TC/SP2019/posters/hotcrp_sp19posters-final33.pdf

Summary:

The basic idea of this research paper is to provide secure QR code as some applications need security within the QR code. In order to design secure QR codes, this research paper proposed a technique of encryption and decryption named Feistel-like encryption scheme which also provides security within the expense of negligible time without any compression.

This paper describes the working of the Feistel-like scheme as it will first refragment the information and change every bit then shuffle the segment and repeat this process 10 times.

The paper also guides the Shuffling process and the key selection such that key is unique for each XOR operation in the Feistel-like scheme. The encryption is a reversible process that is used to decrypt the information from it. The Decryption process will take only 1/3rd time of the encryption process.

The paper also describes the basic structure of the QR Code and the error codes which prevent against some bit corruptions.