https://doi.org/10.33778/kcsa.2023.23.1.055

큐싱(Qshing) 공격 탐지를 위한 시스템 구현

신 현 창*, 이 주 형**, 김 종 민***

요 약

QR Code는 사각형 모양의 흑백 격자무늬에 데이터를 넣은 매트릭스 형식의 2차원 코드로 최근 다양한 분야에서 활용되고 있다. 특히, COVID-19 확산방지를 위해 누구나 간편하게 사용할 수 있는 QR Code를 활용하여 이동경로를 파악함으로써, 사용량이 급증하게 되었다. 이렇게 QR Code의 사용이 보편화됨에 따라 이를 악용한 큐싱(Qshing) 공격에 대한 피해가 증가하고 있다. 따라서 본 논문에서는 큐싱(Qshing) 공격 탐지 시스템을 구현하여 QR Code 스캔 시 유해 사이트로의 이동 및 악성코드 설치를 탐지하여 개인정보유출을 미연에 방지할 수 있는 기술을 제안하였다.

System implementation for Qshing attack detection

Hyun Chang Shin*, Ju Hyung Lee**, Jong Min Kim***

ABSTRACT

QR Code is a two-dimensional code in the form of a matrix that contains data in a square-shaped black-and-white grid pattern, and has recently been used in various fields. In particular, in order to prevent the spread of COVID-19, the usage increased rapidly by identifying the movement path in the form of a QR code that anyone can easily and conveniently use. As such, Qshing attacks and damages using QR codes are increasing in proportion to the usage of QR codes. Therefore, in this paper, a system was implemented to block movement to harmful sites and installation of malicious codes when scanning QR codes.

Key words : QR Code, QR Scanner, Phishing, Qshing, detection system

접수일(2022년 11월 30일), 수정일(2023년 03월 17일), 게재확정일(2023년 03월 31일)

* 동신대학교 정보보안학과 학부생(주저자)
** 동신대학교 정보보안학과 학부생((공동저자)
*** 동신대학교 정보보안학과 교수(교신저자)

1. 서 론

전 세계적으로 COVID-19가 전파되면서 각국들은 COVID-19의 전염성이 다른 바이러스보다 전파 속도가 빠른 것으로 확인되었고, 이를 통해 COVID-19의 확산방지를 위한 제도들을 빠르게 도입하였다. 국내에서는 이런 COVID-19의 전염 및 이동경로에 대해 파악하기 위해 누구나 간편하게 사용할 수 있는 QR Code를 도입하여 이동경로를 파악하였다. QR Code의 경우 2차원 코드를 사용하여 1차원 바코드에 비해 많은 양의 데이터와 정보를 넣을 수 있고 오류 복원이 쉬운 장점이 있으며, 별도의 스캐너 없이 스마트폰과 같은 개인 단말기를 이용해 쉽고 빠르게 QR Code 속 데이터를 확인할 수 있다는 점에서 사용되어 졌다[1][2][3].

하지만 이러한 QR Code는 일반인들도 누구나 쉽게 만들 수 있고, 특정 정보를 탈취하려는 공격자가 악성코드 설치 및 유해 사이트를 유도하는 주소를 삽입하여 제작하게 된다면, 일반인들은 아무것도 모르고 개인정보유출에 노출될 수 있다. 이런 QR Code의 특징을 악용하는 방식의 공격을 큐싱(qshing)이라고 한다.

본 논문에서는 큐싱(qshing)의 의미와 세부적인 침해 경로를 알아보고 이를 바탕으로 QR Code 스캔 시 유해 사이트로의 이동 및 악성코드 설치를 탐지하여 개인정보유출을 미연에 방지할 수 있는 기술을 제안한다.

2. 이론적 배경

2.1 QR 코드(qr code)

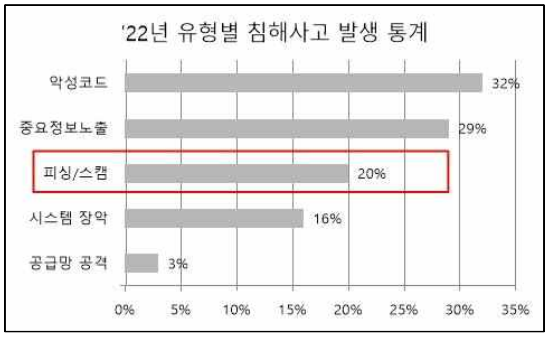
QR 코드(quick response code)는 1994년 일본의 DENSO WAVE 사가 개발한 고속 판독용 매트릭스 2차원 코드를 의미하며, 한 줄로만 자료를 기록할 수 있는 바코드와는 다르게 QR 코드는 매트릭스 형태로 정보를 기록할 수 있다. 한 방향으로만 데이터를 입력, 인식할 수 있는 1차원 바코드와는 다르게 2차원 바코드인 QR 코드는 수평, 수직 방향으로 데이터를 입력, 인식할 수 있으며 이를 통해 숫자와 문자, 특수문자 외에 이미지나 영상 등 더 많은 종류의 데이터를 입력할 수 있게 되었다. 또한, QR 코드의 세 모서리에 배치된 위치 검출 패턴을 통해 코드의 위치를 파악함으로써 모든 방향에서도 빠른 디코딩 및 판독이 가능하도록 설계되었다[4][5].

<표 1> QR 코드의 종류[6]

모델 1 모델 2	Micro QR 코드	iQR 코드	SQRC	Frame Qr
				

2.2 피싱(phishing)

피싱(Phishing)은 개인정보(private Data)와 낚시(Fishing)의 합성어로, 해커가 만든 가짜 금융기관 및 공공기관 웹사이트나 정상적인 메일로 위장한 해킹메일을 이용해서 개인정보 및 금융정보 등을 불법적으로 알아내는 사이버 범죄 기법이다[7].

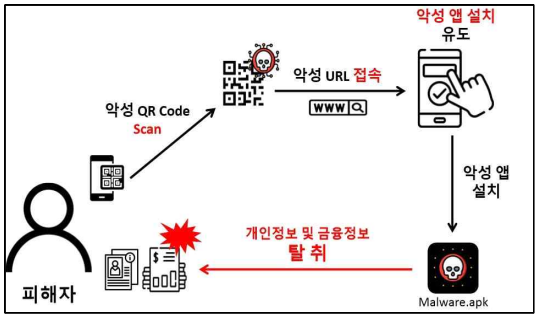


(그림 1) '22년 유형별 침해사고 발생 통계[8]

'EQST 2023 보안 위협 전망 보고서' 의 "22년 유형별 침해사고 발생 통계"에 따르면 피싱 공격은 지난 '22년 한 해 동안 일어난 침해사고 중 20%의 비중을 차지할 만큼 발생 빈도수가 높았다. 특히 사회적 이슈를 악용한 피싱/스캠 공격이 증가하였고 이를 악용해 2차 피해까지 유발시키는 등 피싱으로 인한 피해가 증가하는 추세임을 알 수 있다[8].

2.3 큐싱(qshing)

큐싱(qshing)은 앞서 기술한 QR Code와 피싱(phshing)의 합성어로, QR Code에 악성 앱 설치를 유도하는 URL, 혹은 유해 웹사이트를 링크한 뒤 정상적인 QR Code인 것처럼 위장하여 사용자들에게 유포, 해당 QR Code를 스캔할 시 개인 및 금융정보 탈취, 모바일 기기 권한 탈취 등을 이용해 사기를 유도하는 신종 사이버 범죄이다. 큐싱은 스캔하기 전까지 명확한 정보를 알 수 없다는 QR Code의 허점을 노렸으며, 사용자의 스마트폰, 태블릿 등 별도의 스캐너가 아닌 개인 단말기로도 QR Code를 인식할 수 있다는 장점을 악용한 공격 기법이다.



(그림 2) 큐싱(qshing)의 공격 과정

(그림 2)는 큐싱의 보편적인 공격 과정을 도식화 한 것이다. 대부분의 큐싱 공격은 악성 QR Code내에 내포된 악성 URL로 접속, 악성 앱 설치 혹은 개인정보 입력을 유도하는 방식으로 이뤄지고,이때 공격자가 유도에 성공하게 되면 피해자의 정보를 탈취할 수 있게 된다.

3. 제안 시스템 구성

큐싱 공격에 사용되는 QR Code를 스캔하였을 때 나오는 피싱 사이트는 실제 사이트와 매우 흡사하여 사용자들은 의심하지 않고 해당 피싱 사이트에서 안내하는 과정을 수행하게 된다.

특히, QR Code를 스캔했을 때 가장 먼저 연결되는 URL로부터 큐싱 공격이 시작된다는 점에 착안하여 본 논문에서는 악성 URL을 우선적으로 차단하는 것을 목표로 두었다.

3.1 시스템 개발환경

본 논문에서 제안한 큐싱 공격 탐지 시스템을 구현하기 위해서는 QR Code를 Scan할 수 있는 Application 형태의 QR Scanner가 필요하다.

다음으로 QR Code에 링크된 URL의 정상·비정상 여부를 판단하기 위한 데이터 비교 분석 서버와 비교 대상 URL 값들을 모아놓은 Database가 필요하다. 아래 표들은 큐싱 공격 탐지 시스템을 구현하기 위해 필요한 개발환경들의 세부사양이다.

<표 2> QR Scanner 개발환경

구분	version
OS	Windows 10
CPU	Intel(R) Core i5-10400 2.90GHz
RAM	8GB
Framework	React-native 2.0.1

<표 3> Android 개발환경

구분	version
기종	Galaxy A8 (2018)
OS	Android 7.0 Nougat
RAM	4GB

<표 4> Data Comparison Analysis Server 개발환경

구분	version
OS	Windows 10
CPU	Intel(R) Core i5-10400 2.90GHz
RAM	8GB
Platform	Node.js
Framework	Express 4.18.2
Language	Javascript

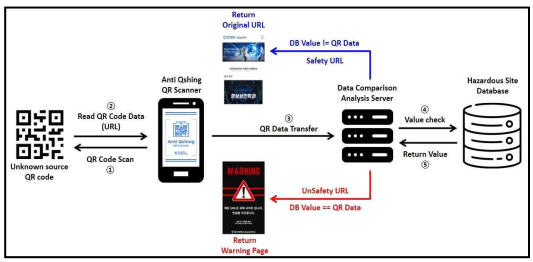
<표 5> Hazardous Site Database Server 개발환경

구분	version
OS	Windows 10
CPU	Intel(R) Core i5-10400 2.90GHz
RAM	8GB
Platform	Cross
Framework	MySQL
Language	C, C++

3.2 큐싱 공격 탐지 시스템 프로세스

큐싱 공격 탐지 시스템의 핵심적인 부분은 자체 개발한 Anti Qshing QR Scanner(QR Code Scanner), QR Code의 데이터를 비교, 분석하는 데이터 비교 분석 서버(Data Compairson Analysis Server), 서버로 전송된 데이터와 비교, 분석에 필요한 악성 URL 데이터가 들어있는 유해사이트 DB(Hazardous Site Database)이다.

(그림 3)은 위 3가지의 핵심적인 부분이 어떻게 동작하고 탐지하여 결과를 도출해 내는지 세부적으로 알 수 있는 큐싱 탐지 시스템 프로세스 구성도이다.



(그림 3) 큐싱 탐지 시스템 프로세스 구성도

다음은 위 구성도의 세부내용이다.

① 사용자는 Anti-Qshing Scanner에 QR Code를 SCAN한다.

② Anti-Qshing Scanner는 인식한 QR Code의 데이터를 읽어온다

③ 이 후, 읽어온 데이터를 데이터 비교 분석 서버로 전송한다.

④ 데이터를 받은 비교 분석 서버는 유해사이트 DB로 전달받은 값과 일치하는 값이 있는지 조회하게 된다.

⑤ 값이 일치할 경우, Hazardous Site로 판단하여 서버에 구성해놓은 Warning Page를 Return 한다.

⑥ 값이 일치하지 않을 겨우, Safety Site로 판단하여 기존의 QR Code URL 값을 그대로 Return 시켜 본래 URL로 접속할 수 있게 한다.

4. 큐싱 공격 탐지 시스템 구현

4.1 Anti Qshing QR Scanner

ReactNative 기반의 자체 개발 QR Scanner로써, 큐싱 공격 탐지 시스템 프로세스 중 QR Code를 Scan해 데이터를 읽어오는 역할을 한다. Android 환경에서 구현이 가능하도록 Framework는 ReactNative를 사용하였고, QR Scanner 구현을 위해 ReactNative의 react-native-qrcode-scanner 라이브러리를 사용하였다.

```
import React, { useState, useEffect } from 'react';
import { StyleSheet, View, Text, Linking } from 'react-native';
import QRCodeScanner from 'react-native-qrcode-scanner';

const Scan = ({navigation}) => {
  const [scanned, setScanned] = useState(false);
  const [cookieValue, setCookieValue] = useState("");
  const [test, setTest] = useState(false)

  return (
    <View style={styles.container}>
      <QRCodeScanner
        onRead={handleQRScanned}
        reactivate={true}
        reactivateTimeout={5000}
        showMarker={true}
        markerStyle={styles.markerStyle}
        bottomContent={
          <Text style={styles.text}>
            {scanned ? '스캔 완료! 확인하려면 새로고침' : 'QR 코드를 인식하세요.'}
          </Text>
        }
      />
      <Text style={styles.cookieText}>{cookieValue}</Text>
    </View>
  );
};
```

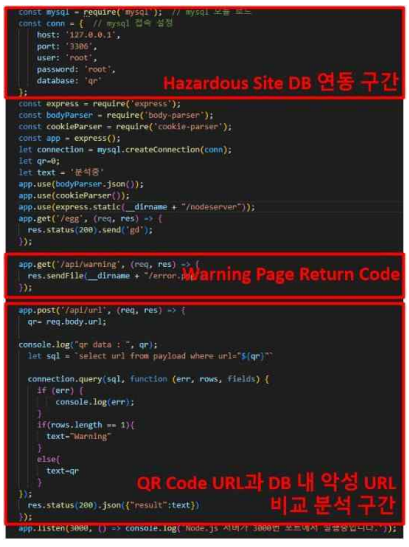
(그림 4) Anti Qshing QR Scanner Source Code

또한, react-navigation/native-stack 라이브러리를 사용해 화면 전환을 구현함으로써 Application의 형태를 완성시켰다. (그림 5)의 좌측은 Anti Qshing QR Scanner의 메인 화면이고, 3초의 Delay 이후 우측의 QR Scanner로 전환되게 구현하였다.

(그림 5) Anti Qshing QR Code Scanner

4.2 Data Comparison Analysis Server

데이터 비교 분석 서버로써, Anti Qshing QR Scanner를 통해 읽어온 QR Code의 데이터를 받고 SQL 구문을 사용해 Hazardous Site DB의 데이터를 조회하여 비교, 분석한 결과 값을 리턴하고 비교 결과에 따라 UnSafety Site로 판단되어질 경우 Warning Page를 Return하는 역할을 하고 있다.



(그림 6) Data Comparison Analysis Server Code

4.3 Hazardous Site DB Server

유해사이트 목록을 저장해놓은 Database 서버이다. Data Comparison Analysis Server로 전달된 후 Hazardous Site DB에 저장되어 있는 URL 값과 비교하여 악성 URL인지 판단하게 된다. (그림 7)은 악성 URL이 저장되어 있는 DB Server이다. 현재 payload table 내에 md5, url 등을 포함한 6개의 컬럼으로 이루어져 있으며, 본 논문에서는 url 컬럼을 주로 사용한다.

(그림 7) Hazardous Site Database

4.4 Qshing Attack Detection

본 절에서는 큐싱 공격 탐지 시스템을 구현한 뒤, 임의로 제작한 2개의 QR Code를 Scan하여 해당 QR Code에 대한 유/무해 여부를 판단하는 테스트를 진행하였다. 테스트는 Galaxy A8, Android OS에서 진행하였다.

먼저 악의적인 행위를 하는 악성 URL을 링크하였다는 것을 가정한 악성 QR Code를 제작한 뒤 Hazardous Site DB에 추가하여 해당 QR Code를 스캔했을 시 악성 URL로 판단하게끔 설정하였고, 다른 하나는 저자의 본교 홈페이지 URL을 링크한 정상적인 QR Code를 제작하였다. 이 후, 자체 개발한 Anti Qshing QR Scanner를 통해 위 2개의 QR Code를 각각 Scan하였으며, <표 4>는 QR Code Scan 이후의 큐싱 공격 탐지 시스템의 구현 결과이다.

정상 URL을 링크한 QR Code의 경우, 큐싱 공격 탐지 시스템의 프로세스에 따라 Safety Site로 판단되어 QR Code에 링크된 정상 URL로 접속하는 것을 확인하였고, 악성 URL을 링크한 QR Code의 경우 Hazardous Site DB에 존재하는 값과 일치하여 UnSafety Site로 판단, 별도의 Warning Page로

이동하는 것을 확인할 수 있었다.

<표 4> 큐싱 공격 탐지 시스템 구현결과

구 분	정상 URL	비정상 URL
QR Code		
결 과		

추가로, 일반 사용자가 앞서 만든 악성 QR Code를 Scan한다고 가정하였을 때 시중에 있는 일반 QR Scanner와 Anti Qshing QR Scanner를 각각 사용해 Scan한 결과를 비교해보았다. 시중에 있는 QR Scanner는 Naver QR Scanner를 사용하였다.

일반 QR Scanner의 경우, 악성 QR Code를 Scan 했을 때 링크해놓은 악의적인 URL로 이동하는 것을 확인하였다. 그러나 Anti Qshing QR Scanner는 해당 QR Code를 Scan 하였을 때 큐싱 공격 탐지 시스템을 통해 UnSafety Site로 판단하여 Warning Page로 이동하는 것을 확인하였다. 만일 해당 QR Code가 테스트용 QR Code가 아닌 실제로 악의적인 행위를 하는 Unknown Source QR Code였다면 QR Code를 스캔했을때 QR Code 내에 있는 악성 URL로 링크되어 개인정보탈취, 악성 앱 설치 및 이로 인한 2차 피해가 발생하는 등 단순한 Scan 한 번으로 사용자는 큐싱의 피해자가 되었을 것이다.

5. 결 론

COVID-19과 펜데믹 상황으로 인해 QR Code 사용률이 급증하였고, 누구나 쉽게 QR Code를 사용하거나 만들 수 있게 되었다. 때문에 어디를 돌아다녀도 어렵지 않게 QR Code를 확인할 수 있고, 누가 만들었는지 모르는 QR Code도 많이 존재한다. 특히 Unknown Source QR Code의 경우, 내부에 어떤 악의적인 행위를 할지 모르는 위험요소가 있기 때문에 인증되지 않은 QR Code는 스캔하지 않는 것이 가장 바람직하다.

본 논문에서는 이러한 문제를 해결하기 위해 큐싱(Qshing)의 공격 기법과 침해 경로에 대해 조사하고 이를 바탕으로 악의적인 URL을 탐지하여 분석하는 큐싱(Qshing) 공격 탐지 시스템을 구현하였다. Anti Qshing QR Scanner를 자체 개발하였고 데이터 비교 분석 서버와 유해사이트 DB를 연동하여 QR Code를 Scan 했을 때, 서버에서 정상·비정상 URL을 분석, 탐지 후 탐지 결과에 따라 정상으로 판단 될 경우 QR Code URL을 그대로 Return 시켜 정상 페이지에 접속할 수 있도록 구현하였으며, 유해 사이트로 판단될 시 Warning Page로 Return 시켜 개인이 유해사이트로의 접속을 차단할 수 있게끔 하였다. 하지만 현재의 시스템은 블랙리스트 기반 탐지 로직을 사용하기 때문에 알려진 유해사이트 및 악성코드에 대해서만 탐지가 가능하다. 추후에는 이러한 단점을 보완할 수 있는 탐지 기술에 대해 제안하여 연구를 진행하고자 한다.

참고문헌

[1] D. W. Kim, Y. T. Jo, and J. M. Kim, "Cloud-based malware QRCode detection system," J. Korea Inst. Inf. Commun. Eng., vol. 25, no. 9, pp. 1227-1233, 2021.

[2] 찐꾸억바오후이, 박상군, 정선태, "발열 감지, 안면 마스크 착용 검출, 전자출입명부QR코드 체킹을 지원하는 보급형 COVID-19디지털 사이니지 플레이어 설계 및 구현", Journal of Korea Multimedia Society Vol. 25, No. 1, pp. 10-28, 2022.

[3] 이은지, 장지경, "QR Code 관련 연구 동향 분석", 한국컴퓨터정보학회 하계학술대회 논문집, 제29권, 제2호, pp.367-368, 2021.

[4] P. S. Jeong, “Smartphone User Authentication Algorithm based on Mutual Cooperation in Mobile Environment”, Journal of the Korea Institute of Information and Communication Engineering, vol. 21, no. 7, pp. 1393-1400, 2017.
[5] Y. J. Park, “Design of Multiple Barcode and QR Code Recognition Systemwith Real-time Object Detection Technology”, Journal of KIIT. Vol. 20, No. 9, pp. 19-30, 2022.
[6] QRcode.com, https://www.qrcode.com/ko/codes/
[7] 김경주, "무역거래의 스피어 피싱 공격에 대한 관리적 대응방안에 관한 연구", 고려대학교 정보보호대학교 석서학위논문, 2019. 02
[8] SK Shieldus, “EQST Annual Report : 2023 보안 위협 전망 보고서”, p. 9, 2023.

〔저자소개〕

신 현 창 (Hyun-Chang Shin)
현 재 동신대학교 정보보안학과 학부생

email : tlsgusckd124@gmail.com

이 주 형 (Ju-Hyung Lee)
현 재 동신대학교 정보보안학과 학부생

email : leejh001219@gmail.com

김 종 민 (Jong-Min Kim)
2015년 산업보안학박사
현 재 동신대학교 정보보안학과 교수

email : dyuo1004@dsu.ac.kr