http://dx.doi.org/10.7236/JIWIT.2012.12.1.83
JIWIT 2012-1-11

QR 코드의 보안 취약점과 대응 방안 연구

A Study of Security Weaknesses of QR Codes and Its Countermeasures

양형규*

Hyung-Kyu Yang

요 약 최근 스마트폰의 보급 확대로 인해 QR 코드의 활용이 급속히 확산되고 있다. 2차원 바코드의 일종인 QR 코드는 간단한 URL이나 명함 등에 폭넓게 사용되고 있으며, 특히 기업의 홍보 수단으로 많이 사용되고 있다. QR 코드는 간단한 사진 촬영으로 정보를 획득할 수 있는 유용한 수단이지만, 한편으로는 의도적인 URL 하이재킹이나 잘못된 정보가 전달될 위험이 있다. 특히 QR 코드는 위변조되더라도 사용자가 인식하기가 거의 불가능하며, 이로 인해 개인정보가 유출되거나 악용될 가능성이 높지만 이에 대한 대책은 전무한 실정이다. 본 논문에서는 이러한 위협에 대해 분석하고 해결할 수 있는 방안을 제시하도록 한다.

Abstract Recently, due to widespread use of smartphones, the number of applications of the QR code is increased rapidly. QR codes, a kind of 2-dimensional barcode, is used to encode information such as simple URLs or namecards, especially for corporates' advertisement. Users can get some information easily by taking picture of the target QR code, however, fake or altered QR codes can cause serious problems, e.g., URL hijacking or infringement of private information because no one can identify the buried information in the QR code by his naked eye. In this paper, I summarize threats to the QR code and present how to tackle these threats.

Key Words : 스마트폰(Smartphone), QR(Quick Response), 보안(Security), 무결성(Integrity)

Ⅰ. 서 론

최근 스마트폰 보급 확대로 인해 QR 코드(Quick Response Codes)의 활용이 급속히 늘고 있다. 스마트폰의 경우 일반 휴대전화와는 달리 다양한 응용프로그램을 자유롭게 설치, 실행할 수 있으며, 내장된 카메라 기능을 이용한 QR 코드 스캐너 프로그램[1,2]이 다양하게 개발되면서 QR 코드를 사용하기 위한 환경이 갖춰진 것이 주요 원인이다.

QR 코드는 주로 상품의 포장지나 광고지에 인쇄되고 있으며, 소비자가 추가 정보를 필요로 할 경우 인쇄된 QR 코드를 스캔하여 해당 웹사이트에 자동 접속할 수 있어 기업체의 홍보 수단으로 각광받고 있다. 이와 함께 개인의 명함에 포함된 정보를 QR 코드로 작성함으로써 상대방이 보다 편리하게 주소록을 자동 입력하도록 하는 용도로도 활용되고 있다 (그림 1 참조).

*정회원, 강남대학교 컴퓨터미디어정보공학부
접수일자 2012.1.5 수정일자 2012.2.5
게재확정일자 2012.2.10

Received: 5 January 2012 / Revised: 5 February 2012 / Accepted: 10 February 2012
*Corresponding Author: hkyang@kangnam.ac.kr
Dept. of Computer-Media Engineering, kangnam university, Korea

그림 1. 가상의 명함에 대한 QR 코드
Fig. 1. QR Code for arbitrary namecard

이렇듯 편리한 기능을 갖춘 QR 코드의 활용이 증가하고 있지만 보안 취약점에 대한 우려도 점차 커지고 있다. 가장 큰 보안 취약점은 QR 코드 내에 포함된 정보의 무결성을 보장할 수 없다는 점인데, 이는 얼마전 많은 사람에게 피해를 입힌 이메일 피싱[3,4]과 유사하다. 이메일 피싱은 정상 사용자가 보낸 것처럼 공격 대상에게 이메일을 발송하여 메일에 포함된 링크를 클릭하도록 유도하고, 실제로 수신자가 링크를 클릭했을 때 전혀 다른 위장 사이트로 연결하여 개인정보나 금융거래에 필요한 비밀번호 등을 입력하도록 하는 수법이다.

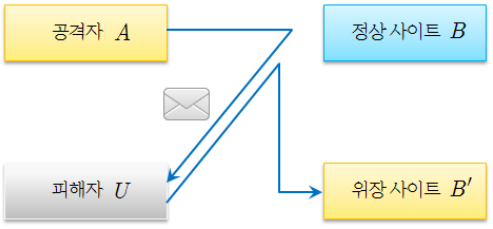

그림 2. 피싱 메일 진행도
Fig. 2. Process of phishing mail

하지만, 피싱 메일의 경우 메일의 내용과 웹브라우저에 표시되는 주소를 주의해서 비교해 보면 어느정도 피해를 예방할 수도 있다. 이에 비해 QR 코드는 사람이 인식할 수 없는 코드이기 때문에 자동으로 연결되는 사이트를 검증하기가 쉽지 않은 문제가 있다. 따라서, 이벤트나 상품 정보를 위한 QR 코드가, 개인 정보를 무단 수집하는 사이트 URL의 QR 코드로 변조되어 있더라도 이를 인지하기 어렵고 특히 해당 QR 코드가 변조되었는지 여부를 검증하는 것은 더더욱 불가능하다.

본 논문에서는 이러한 QR 코드에 대한 보안 위협에 대해 설명하고 이를 해결할 수 있는 방안을 제시하도록 한다. 먼저 2 장에서는 QR 코드에 대해 설명하고 3 장에서는 무결성을 중심으로 QR 코드에 대한 보안 위협을 설명한다. 그리고 4 장에서 이에 대한 해결 방안을 살펴보고 5 장에서 제안한 방식의 장단점을 비교한 후, 마지막으로 6 장에서 결론을 맺도록 한다.

II. QR 코드

1. 개요

QR 코드는 Quick Response의 약자로서, 1994년 일본의 덴소사에 의해 개발된 2차원 바코드이다[5]. 기존 1차원 바코드의 정보량 제한을 해결하기 위해 2차원으로 확장함으로써 저장할 수 있는 정보량을 획기적으로 증가시킨 반면 물리적으로 차지하는 공간은 축소시킨 장점이 있다. 1차원 바코드의 경우 다수의 수직선으로 구성되어 있으며 수직선의 굵기와 간격을 이용하여 데이터를 표현하기 때문에 선형 또는 1차원 바코드라고 부르며, 1차원 고밀도 바코드인 Code 128인 경우 ISO/IEC 15417(2007)[6]로 표준화되어 있으며, 바코드 검증기는 ISO/IEC 15426-1(2006)[7]로 표준화되어 있다. 다음 그림은 "barcode" 문자열을 Code 128로 인코딩한 결과이다.

그림 3. Code 128 바코드 예제
Fig. 3. Example of Code 128 BarCode

QR 코드는 1차원 바코드보다 훨씬 많은 데이터를 기록할 수 있는데, QR 코드로 표현할 수 있는 데이터량의 최대값은 표 1과 같다.

표 1. QR 코드 데이터 용량
Table 1. QR code data capacity

데이터 종류	용 량 (최대)
숫자	7,089 문자
숫자 + 알파벳	4,296 문자
바이너리(8비트)	2,953 바이트
한자	1,817 문자

QR 코드는 2000년 6월에 ISO/IEC18004로 국제표준으로 채택[8] 및 2006년 개정[9]되었으며, 국내에는 2007년 10월 KS 규격으로 제정[10]되었다.

2. QR 코드의 구성

QR 코드는 위치 심볼, 정렬 심볼, 버전 정보, 포맷 정보와 함께 데이터 및 오류 정정 키로 구성되어 있다 (그림 4 참조).

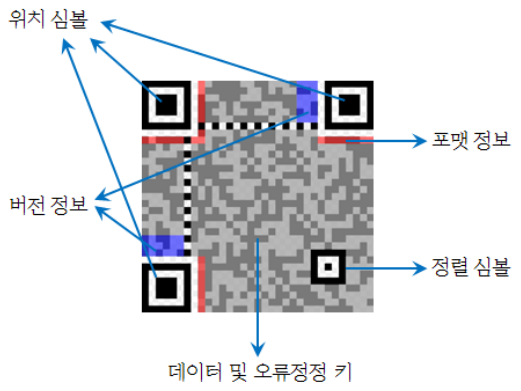

그림 4. QR 코드의 구성
Fig. 4. QR code structure

3. QR 코드의 종류

QR 코드는 저장 용량에 따라 21x21 크기의 버전 1부터 177x177 크기의 버전 40까지 40 개의 버전으로 구성되어 있으며, 특히 위치 심볼이 하나인 마이크로 QR 코드도 제공하여 활용도를 높이고 있다.

각각의 버전은 4가지의 오류 복원 수준에 따라 저장 용량이 결정되는데, 가장 많은 데이터를 보관할 수 있는 버전 40에서, 오류 복원 수준에 따른 바이너리 데이터 저장 용량의 변화는 다음 표와 같다.

표 2. 버전 40의 용량
Table 2. Data capacity of version 40

오류 복원 수준	용 량 (최대)
L	2,953 바이트
M	2,331 바이트
Q	1,663 바이트
H	1,273 바이트

Ⅲ. QR 코드의 보안 취약점

1. 코드 위·변조 공격

QR 코드 내에는 수록된 정보의 오류를 정정하기 위한 코드가 포함될 수는 있지만 이러한 오류 정정 기능을 코드의 무결성을 검증하는데 사용할 수는 없다. 왜냐하면 코드 자체를 다른 코드로 대체하거나 오류 정정 코드 부분까지 바꿀 수 있기 때문이다.

QR 코드는 공개된 기술이고 매우 적은 공간에 많은 정보를 기록할 수 있기 때문에, 스마트폰 확산과 더불어 제품에 대한 추가 정보 사이트를 안내하거나 홍보용 이벤트 등의 용도로 폭넓게 사용되고 있다. 특히 오프라인 인쇄 매체는 물론이고 온라인 사이트에서도 QR 코드를 이용하고 있는데, 만약 이러한 QR 코드가 해킹 등으로 인해 다른 QR 코드로 변조될 경우 변조 여부를 쉽게 확인할 수 없기 때문에 피싱 메일의 경우처럼 전혀 다른 사이트로 연결됨에도 불구하고 이를 파악하기 쉽지 않은 문제가 있다. 오프라인 출력물인 경우 변조된 QR 코드를 덧붙이기만 하면 되기 때문에 더욱더 손쉽게 공격의 대상이 될 수 있다 (그림 5 참조).

그림 5. QR 코드 변조를 이용한 공격
Fig. 5. Attack by modification of the QR code

특히, 사용자 입장에서는 QR 코드를 스캔하여 접속한 사이트를 신뢰할 수 밖에 없기 때문에 문제가 더욱 심각하다. 예를 들어, 이벤트 안내 인쇄물에 이벤트 내용이 적혀 있고, 참여를 원할 경우 QR 코드를 스캔하라고 했다

면, 대부분의 사용자는 별다른 의심없이 QR 코드를 스캔하게 되고 이를 통해 접속한 사이트도 신뢰하게 되지만 정상 사이트가 아닌 해킹 사이트에 접속할 경우 개인 정보 유출 등의 문제가 발생할 수 있다. 또한, 유사한 공격 방법으로 악성 소프트웨어의 설치를 유도할 수 있으며, 이를 통해 휴대폰에 저장된 각종 중요 정보가 유출될 경우 심각한 피해를 입을 수도 있다.

2. 악성코드 공격

QR 코드의 내용은 육안으로 식별할 수 없고 디코딩 과정을 거쳐 확인하기 때문에 주의할 필요가 있다. 특히 많은 디코딩 소프트웨어는 QR 코드 스캔 결과가 사이트 URL인 경우 사용자 편의를 위해 자동으로 해당 사이트에 연결시키는데 이는 의도하지 않은 결과를 초래할 수 있다. 예를 들어, 해당 사이트가 악성 프로그램의 설치를 유도하거나, 특정 사이트에 대한 취약점을 이용하여 공격하도록 만들 수도 있다. 만약 QR 코드 스캔 후 악성 소프트웨어를 설치하였다면 3.1절에서 설명한 코드 위·변조 공격의 경우처럼 매우 심각한 결과를 초래할 수 있다.

이 공격은 사용자로 하여금 악성 URL을 이용하도록 한다는 점에서 코드 위·변조 공격과 유사하지만 정상적인 QR 코드를 위조하거나 변조하는 것이 아니고 사용자의 궁금증을 유발하여 스캔하도록 하며, 처음부터 정상 사이트가 존재하지 않는다는 점에서 다소 차이가 있다. 만약 다수의 사용자가 이러한 악성 QR 코드를 스캔하게 된다면 DDoS 공격으로까지 이어질 수 있다 (그림 6 참조).

그림 6. 악성 QR 코드를 이용한 공격
Fig. 6. Attack using a malicious QR code

Ⅳ. 대응 방안

본 장에서는 3 장에서 살펴본 두가지 공격 유형에 대한 두가지 대응 방안으로, 통합 URL 검증 사이트를 이용하는 방안과 QR 코드의 무결성 검증 및 인증 방안에 대해 설명하도록 한다.

1. 통합 URL 검증 사이트

통합 URL 검증 사이트는 스캔 결과값을 악성 URL 데이터베이스와 비교한 후 정상적인 URL로 판정한 경우에만 연결하도록 하는 사이트를 의미한다. 구체적인 실행 과정은 다음과 같다 (그림 7 참조).

1. 사용자 : QR 코드 스캔
2. 스캐너 : 코드 스캔 결과 URL인 경우 검증 사이트에 URL 전송
3. 검증 사이트 : 악성 URL 목록과 비교하여 결과 전송
4. 스캐너 : 악성 URL이 아니면 Redirection 처리하고 악성 URL이면 차단

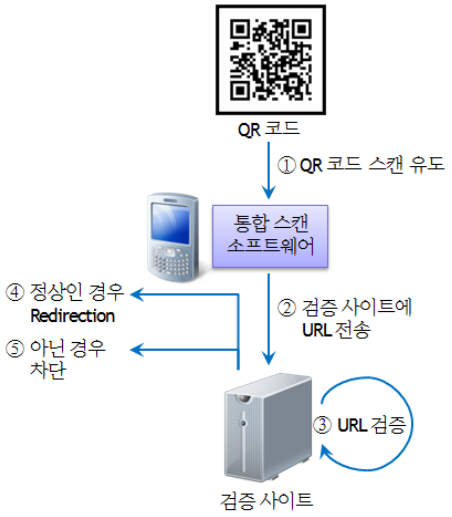

그림 7. 통합 URL 검증 사이트 이용
Fig. 7. Usage of an integrated URL validation site

이 방법은 3장에서 설명한 두가지 공격에 효율적으로 대처할 수 있지만, 모든 사용자가 특정 스캐너(디코더)를 이용해야 하고, 모든 악성 URL을 데이터베이스화하기 쉽지 않다는 문제가 있다. 특히 알려지지 않은 악성 URL인 경우 정상적으로 Redirection 되기 때문에 사용자로

하여금 악성 사이트를 신뢰할 수 있는 사이트로 인식하게 할 우려가 있다.

2. QR 코드의 무결성 검증 및 인증

이 방법은 두 개의 QR 코드를 필요로 하는데, 첫 번째 QR 코드에는 URL과 같은 정보가 포함되어 있으며 두 번째 QR 코드에는 첫 번째 QR 코드에 대한 인증값을 포함하도록 하는 방안이다. 이 방법에서 사용하는 용어는 다음과 같다.

- QR_i : 정보 i에 대한 QR 코드
- $S()$, $V()$: 전자서명 생성 함수 및 검증 함수
- $Cert_A$: 공인인증기관에서 발급한 A의 인증서
- $Cert$: 공인인증기관의 인증서

무결성 검증과 인증을 위한 QR 코드 생성 과정을 다음과 같다. 먼저 A는 공인인증기관으로부터 자신의 인증서 $Cert_A$를 발급받고, QR 코드로 표현하기 위한 정보 I를 생성한다. I는 URL이 될 수도 있고 기타 다른 정보일 수도 있다. 그런 다음 $\sigma = S(I)$를 계산한 후 $i = I \| \sigma \| Cert_A$에 대한 QR_i를 생성한다. 다음 그림 8은 이러한 인증 QR 코드 생성 과정을 그림으로 나타낸 것이다.

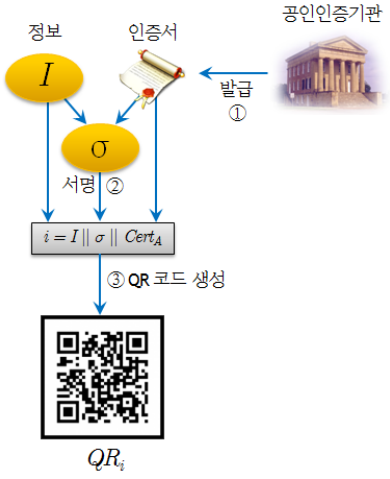

그림 8. 인증 QR 코드 생성
Fig. 8. Generation of an authenticated QR code

이 QR 코드에 대한 사용자 검증 과정은 다음과 같다. 먼저 코드를 스캔 및 디코딩하여 $i = I \| \sigma \| Cert_A$를 얻는다. 그리고 공인인증기관의 인증서인 $Cert$를 이용하여 $Cert_A$의 유효성을 검증한다. 만약 $Cert_A$가 유효하다면 $Cert_A$를 이용하여 서명값 σ가 I에 대한 서명으로 유효한지 검증한다. 검증에 통과하면 정보 I는 A가 생성한 정보이고, 위·변조되지 않았음을 확신할 수 있지만, 그렇지 않다면 위·변조된 정보이므로 처리하지 않는다 (그림 9 참조).

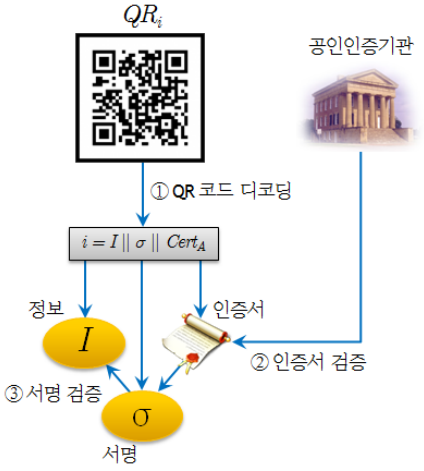

그림 9. 인증 QR 코드 생성
Fig. 9. Generation of an authenticated QR code

V. 효율성 검토

본 장에서는 4장에서 제시한 두가지 해결 방법에 대한 효율성을 분석해보도록 한다.

1. 통합 URL 검증 사이트

먼저 통합 URL 검증 사이트를 이용할 경우 앞에서 설명한 두가지 공격을 모두 막을 수 있다. 하지만, 이를 위해서는 잠재적인 악성 URL을 포함하여 모든 악성 URL을 확인할 수 있어야 하는데, 이는 현실적으로 매우 어려운 문제이다. 만약 악성 URL을 효율적으로 식별할 수 없다면 사용자에게 정확한 정보를 줄 수 없기 때문에 오히려 더 위험한 결과를 초래할 수도 있다. 다만, 악성 URL을 효율적으로 확인할 수 있다면 사용자 단말의 연산 부

담이 거의 없기 때문에 연산 효율성이 매우 높으며, QR 코드를 생성하는 입장에서도 추가적인 연산이나 준비가 필요없다는 장점이 있다.

2. QR 코드의 무결성 검증 및 인증

두 번째 방법으로 제시한 QR 코드의 무결성 및 인증 방법을 통해서도 두가지 공격을 모두 막을 수 있다. 하지만 다음 두가지 사항을 검토해야 한다. 먼저 i로부터 QR_i를 생성할 수 있는지의 문제이다. 즉, i의 크기가 QR를 생성할 수 있을 정도인지의 문제인데, QR 코드가 수용할 수 있는 데이터는 최대 2,953바이트이고, 인증서의 일반적인 크기가 1,500바이트 내외, 그리고 서명값은 256바이트(=2,048비트)이기 때문에 약 1,000바이트의 정보를 수용할 수 있어 URL 등의 간단한 정보를 포함하기에 충분하다고 할 수 있다. 또한, QR 코드는 두 개 이상의 코드를 연속해서 생성할 수 있기 때문에 이보다 긴 정보도 충분히 수용할 수 있다.

또 다른 문제는 $Cert_A$를 검증하는 문제이다. 이는 두가지 방법이 있다. 하나는 온라인을 통해 공인인증기관에 접속하여 검증하는 방법이고, 다른 하나는 사용자의 단말에 공인인증기관의 인증서를 설치하는 방법이다. 두 방법 모두 현실성이 떨어지거나 비효율적인 문제는 없기 때문에 어느것을 적용해도 무방할 것으로 생각된다.

이 방법의 단점은 인증서 검증 등으로 인해 사용자 단말의 연산 부담이 높다는 점이다. 물론 인증서 검증을 온라인으로 처리할 수도 있지만, 사용자 단말에서는 서명 검증 등의 추가 연산이 필요하다. 또한 인증 QR 코드 생성시 인증서를 발급받아야 하고 서명을 생성해야 하는 등의 연산량 증가도 단점으로 생각할 수 있다. 하지만, 통합 URL 검증 사이트를 이용하는 방법은, 현실적으로 모든 악성 URL을 정확하게 판단할 수 있는 방법이 없다는 치명적인 단점이 있어 QR 코드의 무결성 검증 및 인증 방법이 최선의 방법이라고 할 수 있다.

이상을 정리하면 다음 표 3과 같다.

Ⅵ. 결 론

QR 코드는 누구나 자유롭게 생성, 검증할 수 있으며 적은 공간에 비교적 많은 데이터를 수록할 수 있다는 점이 장점이다. 특히, 스마트폰의 보급 확대로 즉석에서 QR 코드를 스캔하고 디코딩할 수 있는 환경이 갖춰지면서 급격하게 보급이 확대되고 있지만, 이로 인해 해커나 악의적인 사용자의 악용 가능성도 함께 제기되고 있다.

본 논문에서는 특히 문제가 될 수 있는 두가지 공격 유형을 설명하였고, 이를 막을 수 있는 두가지 방법을 제시하였다. 두 방식 모두 장・단점을 갖추고 있지만, 현실적으로 모든 악성 URL을 판단할 수 있는 방법이 없기 때문에 기존 PKI와 연동할 수 있는 무결성 검증 및 인증 방법을 최선의 대응책으로 제시하였다.

표 3. 효율성 비교 결과
Table 3. Comparison results of efficiency

		통합 URL 검증 사이트	QR 코드의 무결성 검증 및 인증
위협 요소	코드 위・변조 공격	해결	해결
	악성 코드 공격	해결	해결
장 점		-사용자 단말의 연산 부담 없음 -코드 생성자의 사전 준비 없음	-공인인증서와 서명 검증을 통한 안전한 URL 확인 -기존 PKI를 그대로 활용
단 점		-악성 URL을 완벽하게 검증할 방법이 없음 -잘못된 판단으로 인해 더 큰 피해를 입힐 수 있음	-사용자 단말의 연산량 증가 -코드 생성자의 사전준비 필요

참 고 문 헌

[1] Scany, http://www.scany.net/kr/
[2] QROOQROO, http://www.qrooqroo.com/viewSupport. do
[3] 이메일 피싱, http://www2.fnnews.com/view?ra=Sent1201m_View&corp=fnnews&arcid=00000922380713&cDateYear=2011&cDateMonth=08&cDateDay=02
[4] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, US-CERT, 2011

[5] QR Code, http://www.denso-wave.com/qrcode/ko/index.html
[6] Information technology - Automatic identification and data capture techniques - Code 128 bar code symbology specification, ISO/IEC 15417:2007, 2007
[7] Information technology - Automatic identification and data capture techniques - Bar code verifier conformance specification - Part 1: Linear symbols, ISO/IEC 15426-1:2006, 2006
[8] Information technology - Automatic identification and data capture techniques - Bar code symbology -- QR Code, ISO/IEC 18004:2000, 2000
[9] Information technology - Automatic identification and data capture techniques - QR Code 2005 bar code symbology specification, ISO/IEC 18004:2006, 2006
[10] 정보기술-자동인식 및 데이터 획득 기술-바코드 기호 사양-QR 코드, KS X ISO/IEC 18004:2007, 2007

※ 본 연구는 2010년 강남대학교 교내연구비 지원 연구임.

저자 소개

양 형 규(정회원)

- 1995년 2월 : 성균관대학교 석사
- 1995년 2월 : 성균관대학교 정보공학과 공학박사
- 1995년 ~ 현재 : 강남대학교 컴퓨터미디어정보공학부 교수
- 1984년 12월 ~ 1990년 2월 : 삼성전자 컴퓨터부문 선임연구원

<주관심분야 : 정보보안, 네트워크 보안, DRM>