스마트폰에서의 QR-Code 보안기법에 대한 연구

변진영, 안요한, 이재웅, 이기영

인천대학교 정보통신공학과

A Study of QR-Code Security Method for Smart Phone

Jin-young Byeon, Yo-han Ahn, Jae-woong Lee, and Ki Young Lee

Dept. of Info & Telecom Engineering, University of Incheon

E-mail : ljw0718@naver.com

요 약

본 논문에서는 현재 스마트폰에서 자주 사용하고 있는 QR-Code에 대해서 악의적인 변형 코드 및 올바르지 않은 URL로의 접속 등에 의해 개인정보 유출 등의 피해를 막기 위한 방법을 연구한다.

QR-Code를 디코딩하여 URL 접속 시에 직접적인 필터링은 어려우므로 접속하기 전 해당 QR-Code를 디코딩하여 나온 결과와 원래의 URL을 비교할 수 있는 서버를 만들어 그 서버에 접속하여 스마트폰 사용자에게 접속 여부를 통지해주는 시스템을 구축해보아 스마트폰 사용자들에게 도움이 되고자 한다.

ABSTRACT

This paper shows the way to prevent the leaking of private information due to malicious codes or connections of invalid URL in QR-Codes, which is used in the present smart-phone. It is difficult to filter out the connections directly with decoding the QR-Codes, so before connecting, we construct servers which compare results of decoding the QR-Codes to a valid URL. The server notifies warning to Smart-phone users if the results were uncertain URLs which did not registered in the server. This paper would help the Smart-phone users to protect their privacy.

키워드

QR-Code, QR-Code Filter, QR-Code URL, Smart Phone Security

Ⅰ. 서 론

최근 모바일 기술의 발전으로 휴대폰의 새로운 기능들이 대두되고 있고 스마트폰을 활용한 다양한 응용들이 활발히 사용되고 있다. 그중에 스마트폰과 관련된 여러 응용에서 QR코드의 활용이 급격히 증가하고 있는 추세이다. QR코드는 초기에 자동차부품 생산관리에 주로 사용되다가 현재는 스마트폰에 탑재되면서 교육, 관광, 축제 등 주로 홍보를 위한 수단으로 영역이 확장되었다. 바코드보다 대용량 데이터를 저장할 수 있고 오류를 복원할 수 있다는 이점으로 인해 많은 분야에서 QR코드의 사용량이 급증하는 가운데 보안에 대한 염려도 조금씩 제기되고 있다.[1] QR코드의 많은 이용과 QR코드의 취약점을 악용하여 보안에 위협을 주고 있는 것이다.

본 논문은 QR코드로 개인정보 보안침해를 당할 수 있는 시나리오를 통해 그 공격방법과 보안 위협에 대한 방어방법을 알아보고 그 방어시스템을 설계하여 구현하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 QR코드로 통해 공격하는 방법과 이를 방어할 수 있는 방법에 대해 기술한다. 3장에서는 방어 시스템을 설계하여 총체적 알고리즘에 대해 기술한다. 마지막으로 4장에서는 결론 및 향후연구를 기술한다.

Ⅱ. QR-Code를 이용한 공격방법 및 방어기법

2.1 공격방법

스마트폰의 사용자가 점점 늘어나면서 QR코드의 이용률 역시 증가하고 있다.[1] 이에 따라 QR코드를 해킹의 하나의 경로로서 악용하여 스마트폰 사용자의 정보보안에 위협을 가하는 사례가 근래에 나타내고 있다.

QR코드를 통한 공격방법을 다음에 나오는 시나리오는 그림1을 토대로 알아본다.[2]

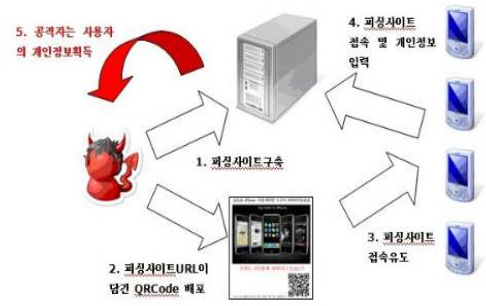

그림 1. QR-Code 이용 공격 기법

해커는 먼저 피싱사이트를 구축하여 피싱사이트 URL이 저장된 QR코드를 웹상에 배포한다. 그 QR코드를 '무료상품(아이패드) 선착순 이벤트'라 사칭하여 일반사용자들이 QR코드에 접속하도록 유도한다. 사용자가 그 피싱사이트로 접속하여 이벤트로 인해 개인정보를 입력하게 될 때에 개인정보는 자연스럽게 해커가 수집하게 된다.

이외에도 QR코드로 통한 공격방법은 많겠지만 패턴은 비슷하다. 악성의 코드를 QR코드에 심어 그로부터 QR코드에 접속한 사용자의 정보를 수집하는 것이다.

2.2 방어방법

위와 같은 공격에 대한 방어방법은 QR코드로 통해 어떤 URL로 접속할 때, 즉각 그 QR코드의 URL로 접속하는 것을 차단하는 것이다. 단지 URL을 화면에 출력해주고 그 사이트의 접속 여부를 물어 사용자 판단아래 접속하는 것이다. 추가로 여러 사이트 주소를 DB에 저장하여 DB의 사이트와 화면에 출력 해준 URL을 비교하여 접속여부를 묻는다. 물론 DB의 사이트는 보안 안전 사이트이다. DB에 사이트가 저장되지 않았다면 사용자의 결정에 따라 접속한다.

Ⅲ. 방어 시스템 설계

QR코드의 이용은 스마트폰으로 이루어짐으로 애플리케이션을 개발하여 악성의 QR코드로부터 보안을 유지한다.

먼저 방어시스템의 알고리즘은 그림 2와 같다.

방어 시스템인 Application을 실행 후 Application에서 QR CODE를 스캔한다. 그 후 스캔한 주소값과 미리 저장된 DB에 있는 값들을 비교, DB에 있는 값과 일치하는 항목이 있다면 그것을 안전값으로 인식하고 사용자에게 알려준다. 알림과 동시에 접속여부를 물어서 접속하면 그대로 접속이 되지만 전단계에서 리스트에 없는 경우 리스트에 없다는 메시지를 출력과 동시에 접속 여부를 물어 접속하지 않는 방향으로 권장한다. 물론 선택은 사용자에 의견에 따른다.

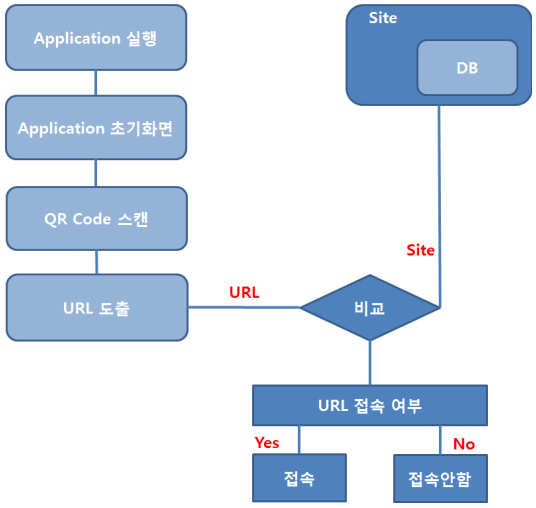

그림 2. 방어 알고리즘

Ⅳ. 결 론

상기의 방법대로 시스템을 구축한다면 고의적인 QR코드 변조 공격으로부터 스마트폰을 방어할 수 있다.

추후에는 QR코드를 스캔 할 때 디코딩 과정에 있어 악의적인 코드를 찾아내는 기법들을 연구하여 서버를 사용하지 않고 독자적으로 QR코드 공격을 막을 수 있는 시스템 설계가 요구된다.

참고문헌

[1] 이경렬, 정만수 "옥외광고에서 QR코드의 활용실태에 관한 연구", 옥외광고학연구 제8권 2호(2011여름) Pp. 61~80

[2] KS X ISO/IEC 18004 : 2007.