CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

QR kodovi i njihova zlouporaba

NCERT- PUBDOC-2012-01-334

Nacionalni CERT

Sadržaj

1 Uvod

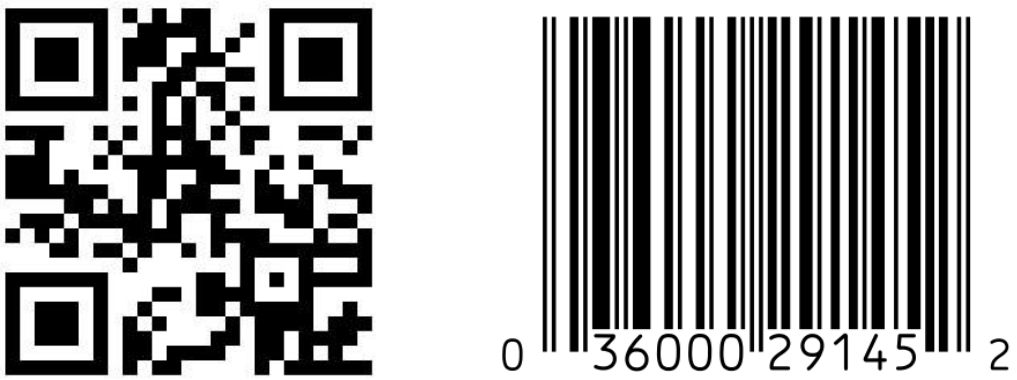
QR kodovi su jedan od najnovijih načina na koji se krajnji korisnici povezuju s određenim sadržajem na globalnoj mreži. Njihova popularnost u zadnjih nekoliko godina naglo je porasla, prvenstveno zahvaljujući pametnim telefonima. Prije pojave novih generacija mobitela, QR kodovi su bili čitljivi samo posebnim laserskim skenerima nepkratičnim za uporabu velikom broju ljudi. Danas je gotovo svaki mobitel ujedno i skener za QR kod. Zbog toga ne iznenađuje činjenica da se QR kodovi pojavljuju na posterima, časopisima, posjetnicama, reklamnim panoima itd. Čitatelju obično nude dodatne informacije, najčešće u obliku poveznica na različita web sjedišta.

Tema ovog dokumenta su zlouporabe QR kodova kao način nanošenja štete vlasnicima mobilnih uređaja. Svijest o postojanju opasnih QR kodova gotovo je nepostojeća kod prosječnih korisnika pametnih telefona. Cilj ovog dokumenta je da razvije tu svijest kroz demonstraciju različitih načina na koje se QR kod može zloupotrijebiti i nanijeti ozbiljnu štetu, bilo putem instalacije malvera na mobilni uređaj ili krađe privatnih podataka.

2 Što je QR kod?

QR kod je vrsta matričnog barkoda dizajniranog za pohranu veće količine informacija od klasičnog jednodimenzionalnog barkoda. Često se naziva i 2D barkod iako taj naziv nije ispravan budući da postoji više vrsta 2D barkodova od kojih je QR samo jedna. Dizajniran je da omogući brzo skeniranje i obradu koda što se očitava i u njegovom nazivu, naime QR je kratica za Quick Response.

Sam barkod je razvila Toyotina tvrtka kćer Denso Wave još 1994. godine. Razvijen je kako bi pomogao u praćenju automobila tijekom procesa proizvodnje, no danas je našao uporabu u različitim područjima ljudske djelatnosti. Iako tvrtka Denso Wave ima patentna prava na QR kod, ona ih ne koristi – QR kod je ISO standard slobodno dostupan svakome.



Slika 2.1 - Usporedba QR koda (lijevo) i klasičnog barkoda (desno)

QR kod ima mnoštvo prednosti nad klasičnim barkodom. U prvom redu tu je veća količina informacija koju može pohraniti. Dok klasični barkodovi mogu kodirati tek nekoliko znamenki, QR kodovi mogu pohraniti od 1000 do 7000 znakova. Točan broj znakova ovisi o vrsti QR koda koji se koristi, ali je svakako daleko više od klasičnog barkoda.

QR kodovi imaju i relativno brzu obradu. Klasični barkodovi su brži zbog svoje jednostavnosti, ali u odnosu na povećani kapacitet QR kodova njihova prednost ne znači puno. QR kodovi su dizajnirani da njihova obrada bude što brža bez obzira na veći kapacitet.

Na kraju valja napomenuti da QR kodovi imaju i veće mogućnosti u ispravljanju pogrešaka. Svaki QR kod može imati različitu razinu ispravljanja pogrešaka, a razine su:

- Low – Omogućuje rekonstrukciju 7% zapisa
- Medium – Omogućuje rekonstrukciju 15% zapisa
- Quality – Omogućuje rekonstrukciju 25% zapisa
- High – Omogućuje rekonstrukciju 30% zapisa

Tako visoke razine ispravljanja pogrešaka omogućuju pravilno čitanje i teško oštećenih QR kodova.

3 Kako QR kod pohranjuje podatke

U ovom dijelu dokumenta ukratko će biti pojašnjen postupak kodiranja podataka u QR kod. Ovo je samo kratak uvod u postupak kodiranja koji je nužno razumjeti kako bi mogli shvatiti zašto QR kodovi mogu biti opasni.

Pogledom na bilo koji QR kod vidimo mnogo crnih i bijelih kvadratića. Oni su osnovni sastavni dijelovi svakog QR koda i u standardu se nazivaju moduli. Kada se neka poruka kodira u obliku QR koda, krajnji rezultat kodiranja je slika sastavljena od modula koji predstavljaju poruku i metapodatke potrebne da se poruka pročita.

Postoji više različitih verzija QR koda koje određuju njegovu veličinu odnosno kapacitet za pohranu informacija. Verzije se kreću od 1 do 40. Verzija 1 označava QR kod veličine 21x21 modula, verzija 2 označava QR kod veličine 25x25 modula i tako sve do verzije 40 koja označava QR kod veličine 177x177 modula.

Verzija nije jedino što određuje ukupni kapacitet QR koda. On ovisi i o vrsti kodiranog sadržaja. Postoji četiri vrste kodiranog sadržaja koji se mogu upisati u QR kod:

- Brojke (numerički sadržaj), maksimalno 7 089 znakova
- Alfanumerički sadržaj, maksimalno 4 296 znakova
- Binarni sadržaj, maksimalno 2 953 znakova
- Japansko pismo, maksimalno 1 817 znakova

Stvarna veličina ovisi o verziji QR koda koji se upotrebljava i o vrsti korekcije pogrešaka.

Svaki QR kod ima nekoliko elemenata koji su zadani i moraju biti prisutni kako bi bio ispravno pročitan. Ti elementi su na sljedećoj slici prikazani u crvenoj boji [1].

Slika 3.1: elementi QR koda

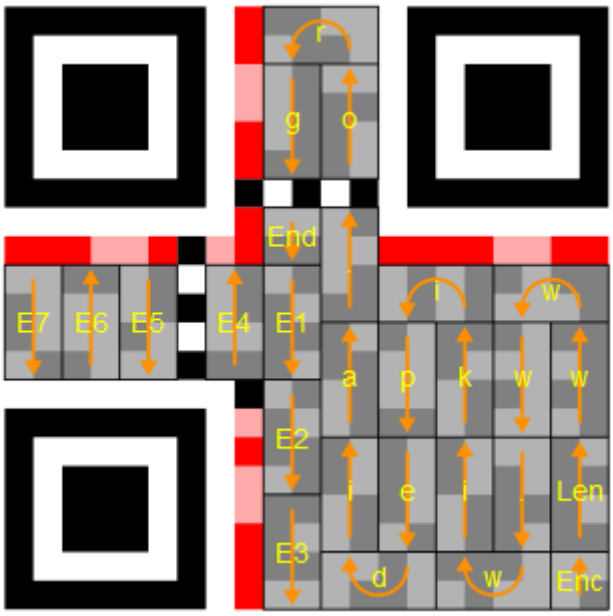
Prvo što se uočava su tri velika kvadrata s bijelim obrubom (na slici je obrub crveni). Svaki kvadrat nalazi se u jednom uglu koda. Oni moraju biti prisutni u svakom QR kodu i skeneru omogućuju da odredi granice koda (širinu i duljinu). Manji crveni kvadrat, koji se nalazi blizu donjeg desnog ruba koda, također služi skeneru kako bi se pravilno pozicionirao za skeniranje koda. Njih može biti i više na jednom QR kodu ukoliko je on veći. Zadnji zadani element su dvije crvene crte koje povezuju po dva velika crvena kvadrata. To su crte koje možemo zapaziti na svakom QR kodu i u njima se izmjenjuju crni i bijeli kvadratići naizmjenično. One također služe skeneru kako bi ispravno pročitao kod.

Plavom bojom na QR kodu je označeno područje u kojem se kodira podatak o verziji QR koda. Isti podatak kodiran je na oba mjesta u obliku binarnog broja gdje crni modul predstavlja broj 1 a bijeli broj 0. Važno je napomenuti da za QR kod verzije ispod 7 nije potrebno kodirati podatak o tome koja verzija koda se koristi.

Dio QR koda označen zelenom bojom rezerviran je za kodiranje podataka o maski koja se koristi i razini korekcije pogrešaka koja se koristi u kodiranju poruke. Taj podatak je kodiran kao jedan binarni broj (crni kvadratići predstavljaju 1, a bijeli 0). Isti broj je kodiran u horizontalnom i vertikalnom smjeru. Maska u QR kodu je zapravo funkcija koja određuje hoće li neki bit poruke biti 1 ili 0 ovisno o njegovoj koordinati unutar QR koda. Prilikom kodiranja poruke, za svaki njezin bit računa se vrijednost maske i ta vrijednost se prikaže kao crni modul ukoliko je 1 ili bijeli ukoliko je 0 na QR kodu. Postoji osam različitih maski za QR kodove. Na maske je najlakše gledati kao na funkcije koje se koriste za upisivanje poruke u QR kod.

Zašto su maske potrebne? Maske osiguravaju „raznolikost" crnih i bijelih modula u kodu. Naime, ukoliko skener naiđe na dugi niz crnih modula može pogrešno pročitati kod. Skeneri su mnogo točniji ukoliko naizmjence čitaju crne pa bijele module. To predstavlja problem ukoliko želimo kodirati poruku koja ima dugi niz jedinica u sebi. Npr. poruka: 10111111111111011111111111111. Zato koristimo maske. One razbijaju dugi niz jedinica na izmjenični niz nula i jedinica budući da u obzir uzimaju i poziciju bita u QR kodu.

Ostatak QR koda rezerviran je za kodiranje same poruke. Kodiranje počinje u donjem desnom uglu i ide prema gore i na lijevo. Najjednostavnije je kodiranje pojasniti na primjeru. Sljedeća slika prikazuje proces čitanja QR koda koji ima kao poruku zapisanu web adresu www.wikipedia.org.



Slika 3.2: primjer QR koda (izvor: [2])

Na slici 3.2 vidimo standardne elemente svakog QR koda koje smo malo prije opisali (veliki kvadrati na rubovima, crte s izmjeničnim crnim i bijelim modulima te crvenom bojom označeni podaci o maski i razini korekcije pogrešaka).

Sama poruka koja je kodirana u QR kodu sastoji se od:

- **vrste kodiranja** (brojke, alfanumerički znakovi...)
- **duljine poruke**
- **poruka**
- **oznaka kraja poruke**
- **korekcijskih kodova**

Svi ovi djelovi se promatraju zajedno kao jedan niz jedinica i nula koje treba upisati u QR kod i na njih se primjenjuje maska. Skener poruku čita dva stupca prema gore do vrha koda, potom dva stupca prema dolje i tako do kraja koda. Na slici je smjer skeniranja označen strelicom. Skener prvo pročita vrstu kodiranja, na slici označeno slovima „Enc“, potom pročita duljinu poruke (na slici označeno slovima „Len“). Zatim se poruka čita znak po znak, budući da je skener prvo pročitao vrstu kodiranja zna kako pročitati svaki znak poruke. U ovom slučaju radi se o alfanumeričkoj poruci gdje se 8 bita koristi za jedan znak. Poruka je: www.wikipedia.org. Nakon poruke skener čita oznaku za kraj i korekcijske kodove.

4 Zlouporaba QR kodova

Više od četvrtine korisnika se na Internet spaja putem neke vrste mobilnog uređaja i vjerojatno je da će u nekom trenutku koristiti QR kod za tipičnu radnju posjeta web sjedištu zapisanog u kodu. Napadači s pojavom popularnih medija bilo kakve vrste, iste vrlo brzo počinju iskorištavati za svoje kriminalne aktivnosti. Iznimka nisu niti QR kodovi.

4.1 Motivacija za zlouporabu

Današnji mobilni uređaji (prvenstveno tzv. pametni telefoni) sadrže veliku količinu osobnih, odnosno povjerljivih podataka o nama. Prema tome, možemo reći da napadačima predstavljaju „zlatni rudnik" preko kojeg mogu izvući informacije koje mogu zloupotrijebiti, najčešće radi financijske koristi.

Motivi tako mogu biti:

- povjerljivi podaci (adresar, podaci o kreditnoj kartici, povjerljivi podaci s društvenih mreža itd.) koje napadač može iskoristiti za krađu identiteta (oponašanje druge osobe) ili (ciljani) phishing
- poslovni kalendari sastanaka i drugi poslovni poslovni podaci koje napadači mogu iskoristiti za nanošenje štete tvrtki (npr. u poslovne svrhe konkurentske tvrtke)
- poruke elektroničke pošte koje se mogu iskoristiti za nanošenje štete tvrtki
- geografska lokacija vlasnika koju napadači mogu iskoristiti za njegovo uznemiravanje, ucjenjivanje i sl.

4.2 Načini zlouporabe

Najjednostavnija dosad zabilježena vrsta zlouporabe QR koda je ubacivanje poveznice (linka) koja vodi na maliciozno sjedište. Takvo web sjedište može, kao i inače, iskorištavati neku od ranjivosti web preglednika na mobilnom uređaju kako bi na uređaj instalirao malver. Kasnije taj malver obično otima povjerljive korisničke podatke i šalje ih napadačima.

Slika 4.1: primjer posjeta web stranici preko QR koda

Važno je upamtiti kako će napadači obično koristiti različite tehnike socijalnog inženjeringa kako bi korisnika naveli na posjećivanje maliciozne web stranice i/ili instalaciju malvera s nje. Obično će web preglednik prije posjeta nekoj stranici, nakon skeniranja QR koda, još upozoriti korisnika želi li otvoriti tu stranicu, no to je ovisno o vrsti preglednika koji se koristi, odnosno ne mora biti pravilo. Tu je još i mogućnost postavljanja (malicioznih) skraćenih URL-ova unutar QR koda iz kojih je nemoguće zaključiti vodi li konačni URL na neku rizičnu web stranicu. Dodatni problem je što mnogi pametni telefoni ne prikazuju cijeli URL kod posjeta određenoj web stranici (koji može biti maliciozan) nakon skeniranja QR koda (prikazano na slici 4.1), što je osobito opasno jer napadačima može olakšati phishing [8].

Proizvođač sigurnosnih rješenja Websense je u siječnju 2012. otkrio [5] pojavu spam e-maila koji sadrži poveznicu na web stranicu s malicioznim QR kodom. Poveznica je vodila na domenu tag.nl u vlasništvu legitimnog servisa za izradu QR kodova iz URL-a na kojeg korisnik servisa želi da QR kod vodi. Kada se navedeni URL (s tag.nl domenom) posjeti, otvara se web stranica s QR kodom, kojeg ako se skenira prosljeđuje web preglednik mobilnog uređaja na web stranicu namijenjenu (vjerojatno ilegalnoj) prodaji Viagre. Web stranica s malicioznim QR kodom prikazana je na slici 4.2.

Slika 4.2: web stranica s malicioznim QR kodom

Kaspersky je u rujnu 2011. otkrio [6] QR kodove koji su vodili na web stranice koje sadrže trojanske konje namijenjene napadu na mobilne uređaje s operativnim sustavom Android. Jednom instaliran, trojanski konj se integrira u OS kao ICQ klijent s ikonom imena „JimmRussia“ te počinje potajno slanje premium SMS poruka koje se naplaćuju po 6 američkih dolara. Googleov mobilni operativni sustav Android se dosad pokazao mnogo ranjivijim od Appleovog iOS-a, iz razloga što Android aplikacijama ne ograničava radnje kao što su slanje SMS poruka, uspostavljanje poziva i dr. Da bi to omogućili na iOS-u, napadači prvo moraju navesti korisnika da svoj uređaj otključa („jailbreaking“) te onda na njega instalira malver.

Napadači također mogu jednostavno zalijepiti lažni (maliciozni) QR kod na originalni te ih proširiti širenjem promidžbenih letaka ili slično. U prosincu 2011. jedna je turistička zajednica u Ujedinjenom kraljevstvu odlučila podijeliti čak 250 000 letaka na kojima su ispisani QR kodovi [4]. Ovaj primjer najbolje dokazuje kakva opasnost prijeti od maloprije spomenute vrste napada, a veća primjena QR kodova tek počinje. Napadači zahvaljujući QR kodovima imaju mogućnost primjene socijalnog inženjeringa izvan računalnog svijeta. Na primjer, mogu isprintati letke koje navode korisnike na skeniranje QR kodova i polijepiti ih po gradskim parkiralištima, a ljudima obećati da će zauzvrat biti nagrađeni besplatnim parkingom i sl.

5 Zaštita

5.1 Nekoliko brzih savjeta

Poznati proizvođač antivirusnih rješenja, AVG, navodi [3] nekoliko mjera kojih se korisnici trebaju pridržavati prilikom upotrebe QR kodova:

- nikad nemojte slijepo vjerovati bilo kojem QR kodu i uvijek im pristupajte s određenom dozom sumnje
- obavezno na svoj mobilni uređaj instalirajte aplikaciju zaduženu za sigurnost; za većinu popularnih mobilnih operacijskih sustava postoje besplatne i komercijalne inačice takvih aplikacija
- ako QR kod vodi na web stranicu koja od vas traži povjerljive podatke poput korisničkog imena, lozinke, bankovnog računa ili sl., vrlo je vjerojatno riječ o prijevari
- ako vas QR odvede na web stranicu gdje se potrebno prijaviti (ulogirati), nemojte se prijavljivati na taj način, nego direktno upišite URL web sjedišta u svoj web preglednik

Uz ove savjete, također je važno redovito vršiti sigurnosno pohranjivanje podataka s mobilnih uređaja (npr. kopiranje na računalo), tako da se oni mogu lako povratiti, u slučaju da uređaj ipak bude zaražen nekom vrstom malvera.

5.2 Usporedba mobilnih aplikacija

Jedna od najvažnijih mjera zaštite mobilnih uređaja je korištenje takve aplikacije za čitanje QR kodova koja će korisnika upozoriti (i tražiti njegovu dozvolu) prije nego što ga preusmjeri na URL iz QR koda. Također, ukoliko QR kod sadrži JavaScript programski kod kojeg treba izvršiti, bitno je da i u tom slučaju korisnik bude pravovremeno (prije izvršavanja koda) upozoren.

AppSec Labs, tvrtka koja se bavi računalnom sigurnošću, provela je testiranje dostupnih aplikacija za čitanje QR kodova [7]. Kao kriterij je uzeta činjenica traže li od korisnika potvrdu kod posjeta URL-ovima iz QR kodova. Drugi kriterij je bio upozoravaju li korisnika da će pokrenuti JavaScript kod, ukoliko imaju mogućnost (ugrađenu funkcionalnost) pokretanja JavaScript koda koji je upisan unutar QR koda. Ovaj test nisu prošle samo dvije

aplikacije, a to su ujedno i jedine aplikacije na testu koje su bile u stanju prepoznati (parsirati) JavaScript kod (koji se nalazi unutar QR koda). Tablica 4.1 daje pregled rezultata testa [7]. Važno je napomenuti kako je moguće da test ne prikazuje trenutačno stanje ukoliko je aplikacija promijenila svoju funkcionalnost. Također neke od navedenih aplikacija dostupne su samo na pojedinim mobilnim operativnim sustavima (Android, iOS itd.)

Tabela 1: usporedba aplikacija za čitanje QR kodova [izvor: AppSec Labs]

Aplikacija	JavaScript test	Test preusmjeravanja na URL
TapReader	Prošao	Prošao
QR+	Prošao	Prošao
QRReader	Prošao	Nije prošao
Scan	Prošao	Nije prošao
RedLaser	Prošao	Prošao
i-nigma	Prošao	Nije prošao
BeeTagg	Prošao	Prošao
QR Code Reader	Prošao	Nije prošao
QuickMark	Nije prošao	Nije prošao
QR+Emoji	Prošao	Prošao
Bakodo	Prošao	Prošao
Optiscan	Prošao	Prošao
QR-Scanner	Prošao	Prošao
quiQR	Prošao	Prošao
QR Code City	Prošao	Ovisno o postavkama
RedLaser eBay	Prošao	Prošao
ATTScanner	Prošao	Prošao
QR Droid Private	Prošao	Prošao
Bakodo	Prošao	Prošao
Posted	Nije prošao	Prošao
NeoReader	Prošao	Prošao

6 Zaključak

Zbog sve veće primjene QR kodova, očekuje se i sve veći broj napada putem njih. Posebno iz razloga što tvrtke poput PayPala planiraju uvođenje servisa za plaćanje putem QR kodova. Ubrzavanjem korisničke interakcije, uvijek se gubi na sigurnosti, a tako je i u ovom slučaju. Važno je prepoznati koje su mogućnosti QR kodova i prihvatiti činjenicu da će oni napadačima poslužiti kao još jedan dodatni vektor napada. Korisnici mobilnih uređaja, svoj uređaj moraju početi poistovjećivati s običnim (stolnim ili prijenosnim) računalom jer su oni danas praktički dostigli njihovu snagu. Drugim riječima, potrebno je biti jednako oprezan prilikom radnji poput otvaranja web stranica, instalacije aplikacija i sl. Prema tome, s korisnikove je strane najsigurnije svaki QR kod koji dolazi iz neprovjerenog izvora automatski smatrati zlonamjernim.

7 Literatura i reference

1. What Is A QR Code And How Does It Work? http://www.youthedesigner.com/2011/09/29/what-is-a-qr-code-and-how-does-it-work/, objavljeno 29. rujna 2011.
2. QR code, Wikipedia, http://en.wikipedia.org/wiki/QR_code
3. AVG (AU/NZ) Cautions: Beware of Malicious QR Codes, http://www.pcworld.idg.com.au/mediareleases/12655/avg-aunz-cautions-beware-of-malicious-qr-codes/ , objavljeno 28. lipnja 2011.
4. North Wales tourism sites to have own special barcode, http://www.dailypost.co.uk/business-news/business-news/2011/12/29/north-wales-tourism-sites-to-have-own-special-barcode-55578-30026595/ , objavljeno 29. prosinca 2011.
5. Spam Emails Link To QR Codes, http://community.websense.com/blogs/securitylabs/archive/2012/01/09/spam-emails-link-to-qr-codes.aspx , objavljeno 9. siječnja 2012.
6. QR Codes Found Sending Users to Site Containing Android Trojan, http://threatpost.com/en_us/blogs/qr-codes-found-sending-users-site-containing-android-trojan-093011 , objavljeno 30. rujna 2011.
7. EvilQR – When QRCode goes bad: Security assessment of mobile QR readers – Updated (30-Nov-2011), https://appsec-labs.com/blog/tag/qrcode , objavljeno 30. studenog 2011.
8. QR code security risks in the car park, http://nakedsecurity.sophos.com/2011/09/14/qr-code-security-risks-car-park/ , Sophos, objavljeno 14. rujna 2011.